Hitachi Solutions Create

HITACHI

Tripwire Enterprise説明資料

株式会社 日立ソリューションズ・クリエイト

目次

HITACHI

1. Tripwire Enterpriseとは

HITACHI

Tripwire Enterpriseとは

Tripwire EnterpriseはFortra社が提供する、**「変更コントロールソフトウェア」**で、サーバー、クライアント、ネットワーク機器などのITインフラに加えられる変更を一元的に、かつ、常に監視・管理するソフトウェアパッケージです。

FORTRA™

Tripwire Enterprise

- 変更検知に特化！
- 変更検知のパイオニアであり
  デファクトスタンダード
- ファイル整合性（FIM）・セキュリティ構成
  情報管理（SCM）のマーケットリーダー

1. Tripwire Enterpriseとは

HITACHI

ＩＴシステムへの徹底した変更管理でセキュリティを可視化し、
改ざん検知、情報漏えい・標的型攻撃対策を強力にサポート

Tripwire Enterprise は、情報セキュリティの三要素（機密性、完全性、可用性）を構成する「完全性」を維持します。
ITシステムの完全性監視によって、セキュリティの強化、コンプライアンスの証明、運用管理の向上という**三つの価値**を実現します。

セキュリティの強化

- Web 改ざん対策
- ファイル整合性監視
- 情報漏えい対策
- ゼロデイ攻撃対策
- セキュリティレベルの可視化

コンプライアンスの証明

- PCI DSS
- J-SOX（IT全般統制）

運用管理の向上

- 可用性の向上
- ログ管理製品との連携

Tripwire Enterpriseは、システムに加えられた
変更を検知することで**セキュリティの強化**と
コンプライアンスの証明と**運用管理の向上**を実現します

Tripwire Enterpriseの視点

「いかに攻撃を防ぐのか」ではなく、
「影響があったのか、なかったのか」
「どういう影響があったのか」の把握にフォーカス

HITACHI

Tripwire Enterpriseが「変更コントロールのデファクトスタンダード」である理由

経済産業省の情報処理推進機構（IPA）において、**「ECサイトの構築時および運用時における最低限満たすべきセキュリティ対策要件」**として、**ファイル整合性監視（FIM）**が必須だと認められています。
Tripwire Enterpriseは**FIMソリューション**および**SCMソリューション**の**マーケットリーダー**です。

クレジットカードの国際カードブランド5社（American Express、Discover、JCB、MasterCard、VISA）共同で策定した情報セキュリティ標準の PCI DSSに要求されるセキュリティ・コンプライアンスの順守のために **FIMの導入が必要です。**
Tripwire Enterpriseを導入することで、PCI DSSのVer4.0の**要件2の一部**、**要件6の一部**、**要件10.5**、**要件11.5**を満たせます。

2. Tripwire Enterprise活用イメージ

HITACHI

Security　データの改ざんを検知

セキュリティ対策には 100 % 確実なものは存在しません。
アンチウイルスソフトやファイアウォール、IDS など外部からの攻撃を予防する手段をとることは
非常に重要です。
しかし、それと同時に万が一被害にあった場合の事後対策も含め
「抑止・予防・検出・回復」というサイクルでのセキュリティ対策を考える必要があります。

Tripwire Enterpriseは、サーバーやネットワーク機器の変更の発生を迅速に検知し、
「誰が、いつ、どのファイルを変更したのか」を通知できます。

HITACHI

Availability　システムの可用性を向上

システム要件の変更やパッチの適用、新しいアプリケーションの導入など、システムには
日々変更が加えられています。
変更作業がシステムに大きな影響を及ぼす可能性があるにもかかわらず
実際には変更管理は作業報告にとどまっているのが現状です。

Tripwire Enterpriseは、意図した変更が的確に実施されたか、
予定外の変更がなされていないかを確認可能です。
抜け穴のない**変更管理プロセス順守を徹底**できます。

HITACHI

Compliance 変更の監査証跡に利用

ITシステム基盤に発生する変更を、その変更の原因を問わず検知・記録します。
必要に応じて、変更情報を多様な切り口から確認できるレポートを容易に作成し、
IT全般統制の有効性証明を支援します。

Tripwire Enterpriseは、変更管理プロセスにおいて、
正しい手続きに従って変更作業が実施されたことを
レポート機能により記録保管できます。
レポートは、**変更の監査証跡として**
内部・外部監査時（SOX対応）に利用できます。

HITACHI

Compliance

PCI DSS 4.0に対応

クレジットカード会員情報の保護を目的とした国際セキュリティ基準（PCI DSS）に関して、新しい基準となるPCI DSS 4.0が2022年3月にリリースされました。

～ PCI DSS 4.0の主な特徴　～
①リスクベースの考え方の取り込み
②昨今のクレジットカード情報漏えいの傾向を踏まえた新要件の追加
③既存要件で求められる対策のさらなる強化

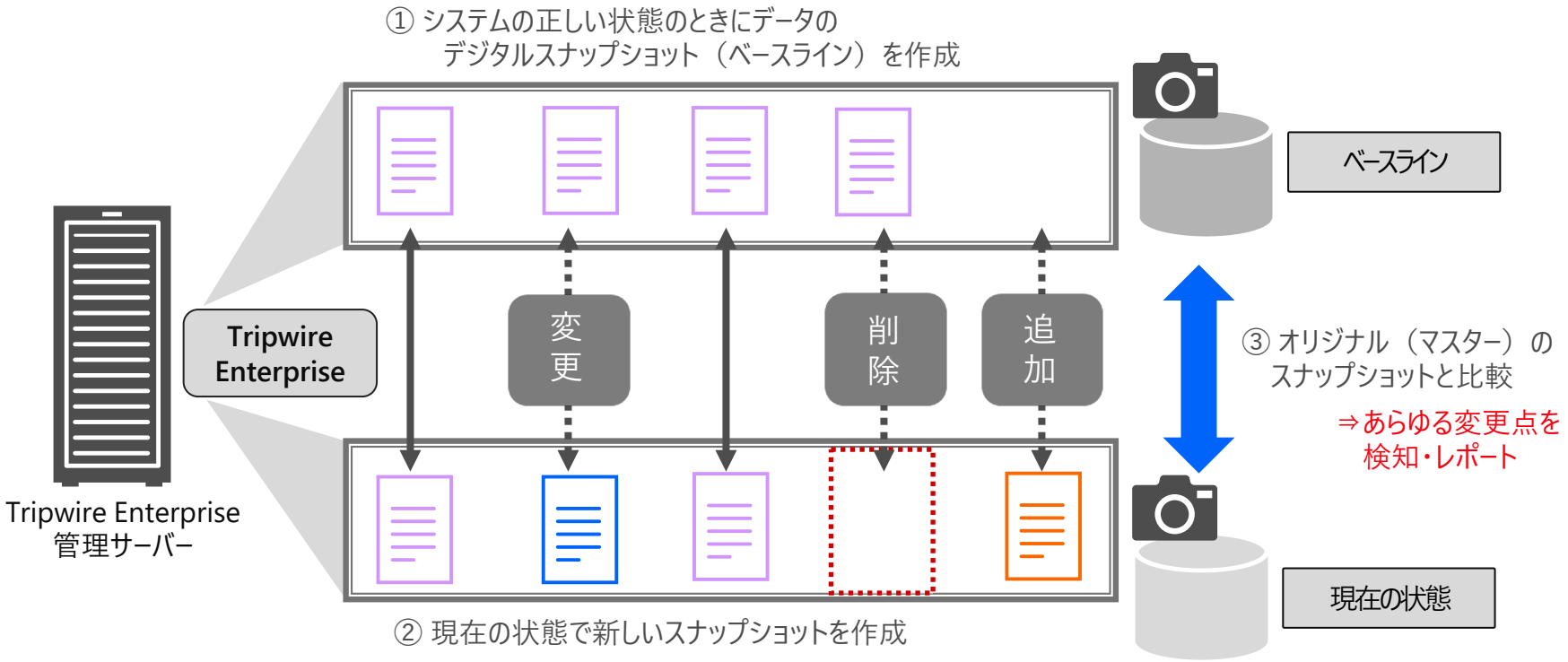
Tripwire Enterpriseは、サポート対象のバージョンにてPCI DSS4.0のポリシーに従ったセキュリティ構成管理ができます。
PCI DSS 4.0をはじめ、CISv2.1.0、ISO、NERC、HIPAAなどのポリシーを提供しています。

3. Tripwire Enterprise製品概要

HITACHI

Tripwire Enterprise - コアテクノロジー

Tripwire Enterpriseは、確認済の最適な状態のファイルや属性のデジタルスナップショットを取得し、**ベースライン**※1を作成します。このベースラインをもとに、自動で変更チェックを行い、ファイルコンテンツの変更やファイルサイズ、アクセスフラグ、書き込み時刻などの**システム属性の変更を検知**し、詳細情報をレポート化します。

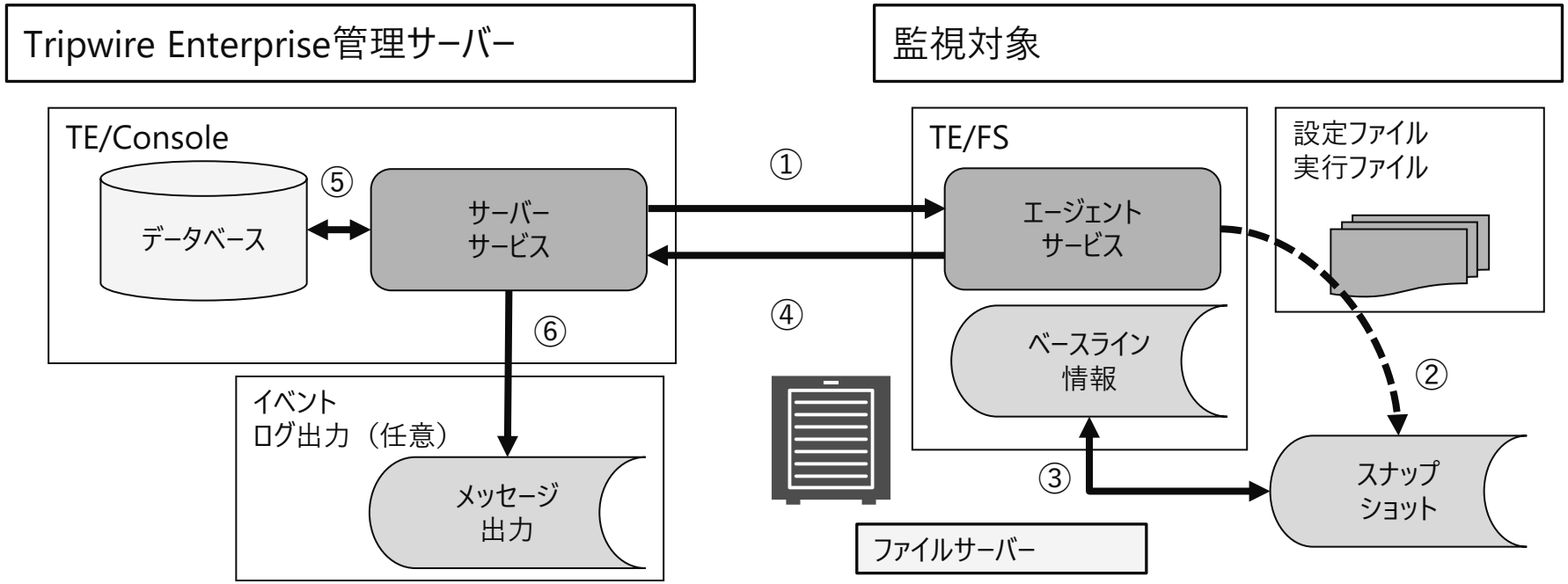


※1：最適な状態のデジタルスナップショット

HITACHI

Tripwire Enterprise - コアテクノロジー

監視対象がファイルサーバーの場合の変更検知機能フロー



①監視対象のサーバーへ変更検知処理の実行を要求

② Tripwire Enterprise管理サーバーで定義された設定に従い、監視対象ファイルの現行のスナップショットを取得

③ベースライン情報との比較

④変更検知結果を送信

⑤監視対象サーバーから送信された変更検知結果をデータベースに登録

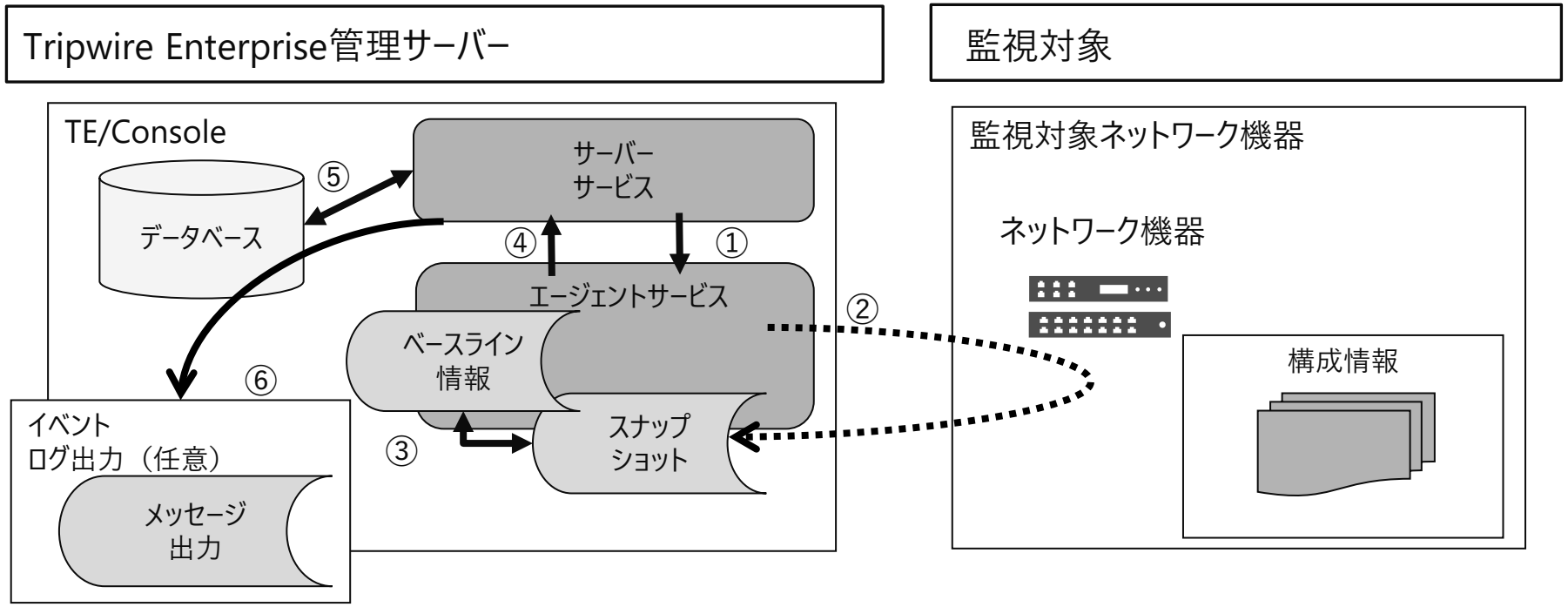
⑥イベントログに変更を検出した旨のメッセージを出力

TE/Console : Tripwire Enterprise Console　TE/FS : Tripwire Enterprise for File System

HITACHI

Tripwire Enterprise - コアテクノロジー

監視対象がネットワーク機器の場合の変更検知機能フロー



①監視対象のネットワーク機器へ変更検知処理の実行を要求

② Tripwire Enterprise管理サーバーで定義された設定に従い、ネットワーク機器にログインし、構成情報の現行のスナップショットを取得

③ベースライン情報との比較

④変更検知結果を送信

⑤送信された変更検知結果をデータベースに登録

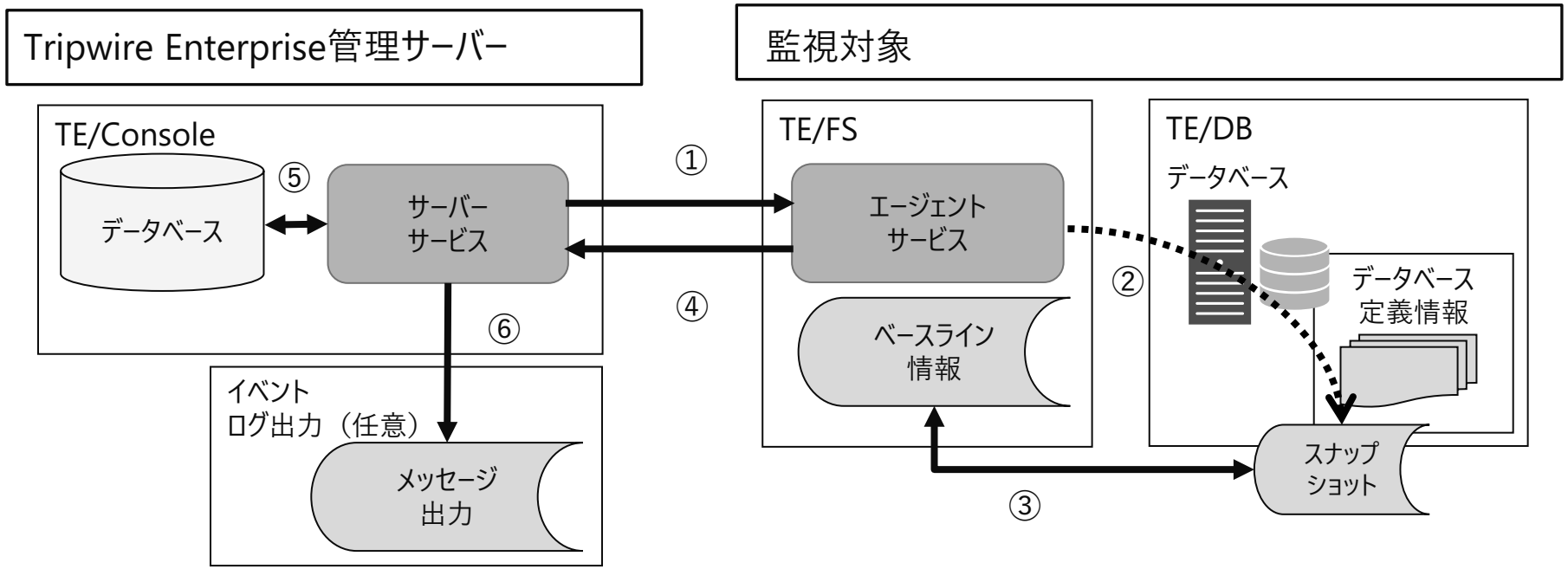
⑥イベントログに変更を検出した旨のメッセージを出力

TE/Console : Tripwire Enterprise Console

HITACHI

Tripwire Enterprise - コアテクノロジー

監視対象がデータベースの場合の変更検知機能フロー



①監視対象のデータベースへ変更検知処理の実行を要求

② Tripwire Enterprise管理サーバーで定義された設定に従い、
TE/FSを介して、データベースにログインし、
構成情報（ユーザー権限、テーブル、ビュー、ストアドプロシージャ）
の現行のスナップショットを取得

③ベースライン情報との比較

④変更検知結果を送信

⑤送信された変更検知結果をデータベースに登録

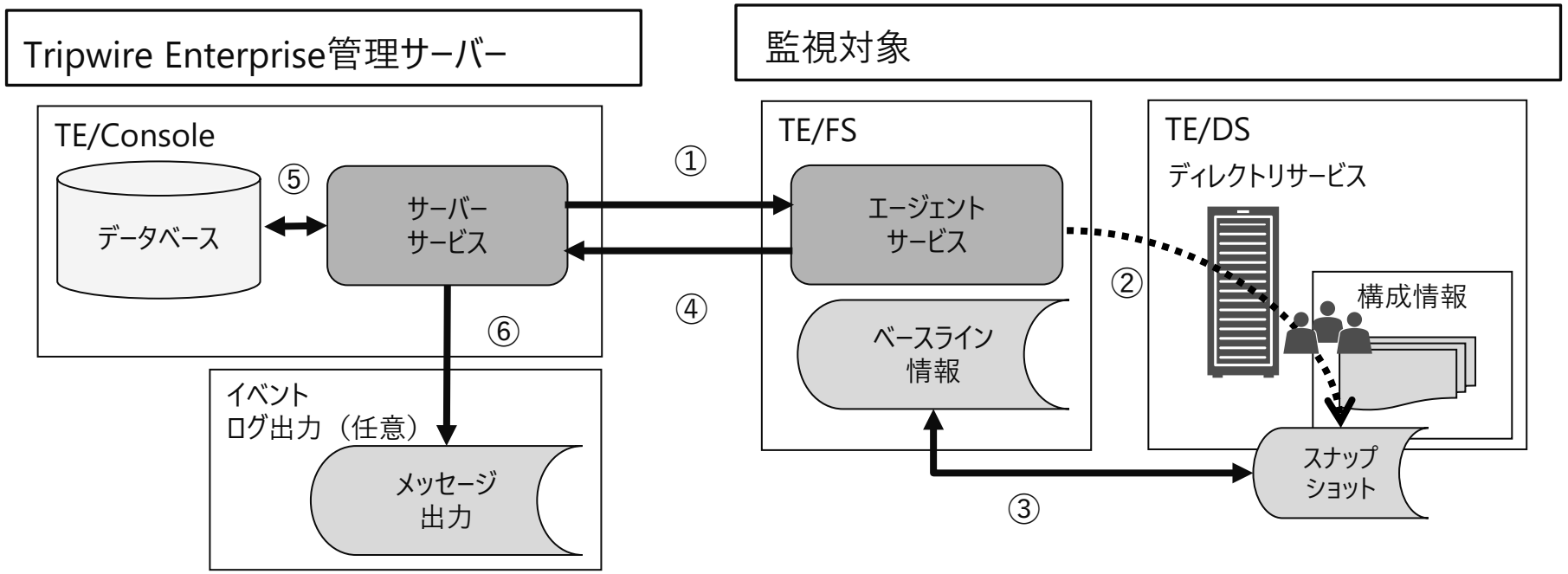
⑥イベントログに変更を検出した旨のメッセージを出力

TE/Console : Tripwire Enterprise Console　TE/FS : Tripwire Enterprise for File System　TE/DB : Tripwire Enterprise for Databases

HITACHI

Tripwire Enterprise - コアテクノロジー

監視対象がディレクトリサービスの場合の変更検知機能フロー



①監視対象のデータベースへ変更検知処理の実行を要求

② Tripwire Enterprise管理サーバーで定義された設定に従い、TE/FSを介して、Active Directoryのスキーマ、パスワード設定、ユーザー権限セキュリティポリシーのオブジェクトや属性の変更など現行のスナップショットを取得

③ベースライン情報との比較

④変更検知結果を送信

⑤送信された変更検知結果をデータベースに登録

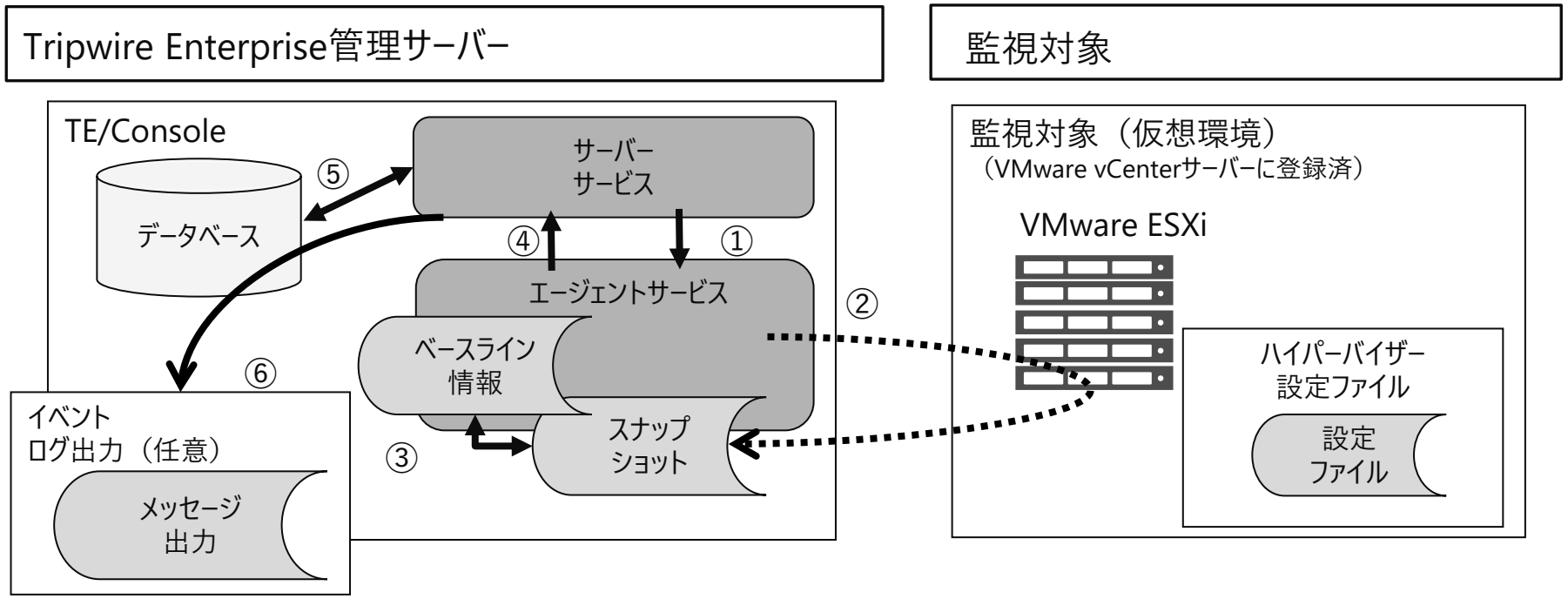
⑥イベントログに変更を検出した旨のメッセージを出力

TE/Console : Tripwire Enterprise Console　TE/FS : Tripwire Enterprise for File System　TE/DS : Tripwire Enterprise for Directory Services

HITACHI

Tripwire Enterprise - コアテクノロジー

監視対象がVMware ESXiの場合の変更検知機能フロー



①監視対象の仮想環境へ変更検知処理の実行を要求

② Tripwire Enterprise管理サーバーで定義された設定に従い、仮想環境にログインし、監視対象ファイル（設定ファイルなど）の現行のスナップショットを取得

③ベースライン情報との比較

④変更検知結果を送信

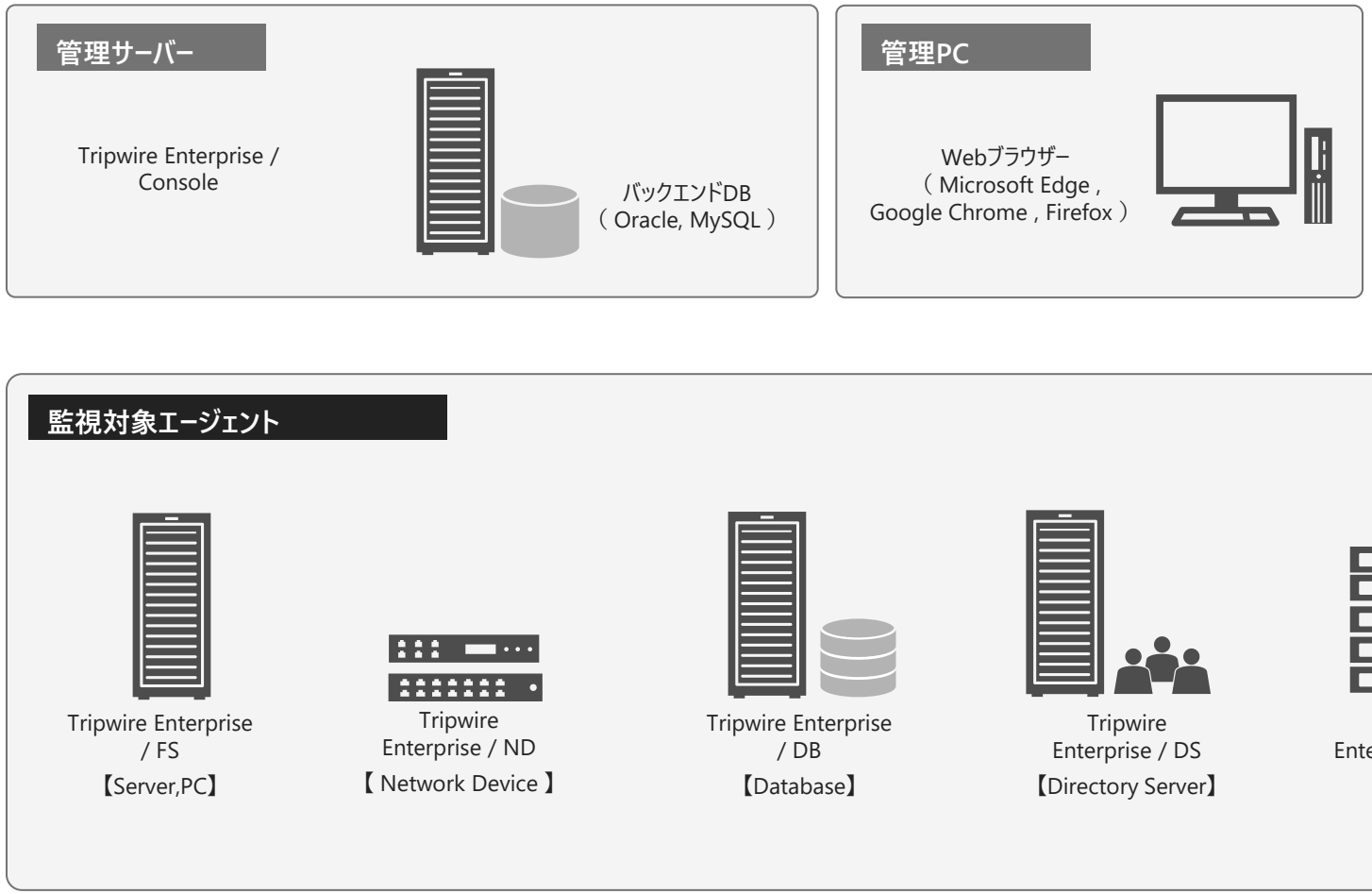
⑤送信された変更検知結果をデータベースに登録

⑥イベントログに変更を検出した旨のメッセージを出力

TE/Console : Tripwire Enterprise Console

HITACHI

Tripwire Enterprise - 製品体系



HITACHI

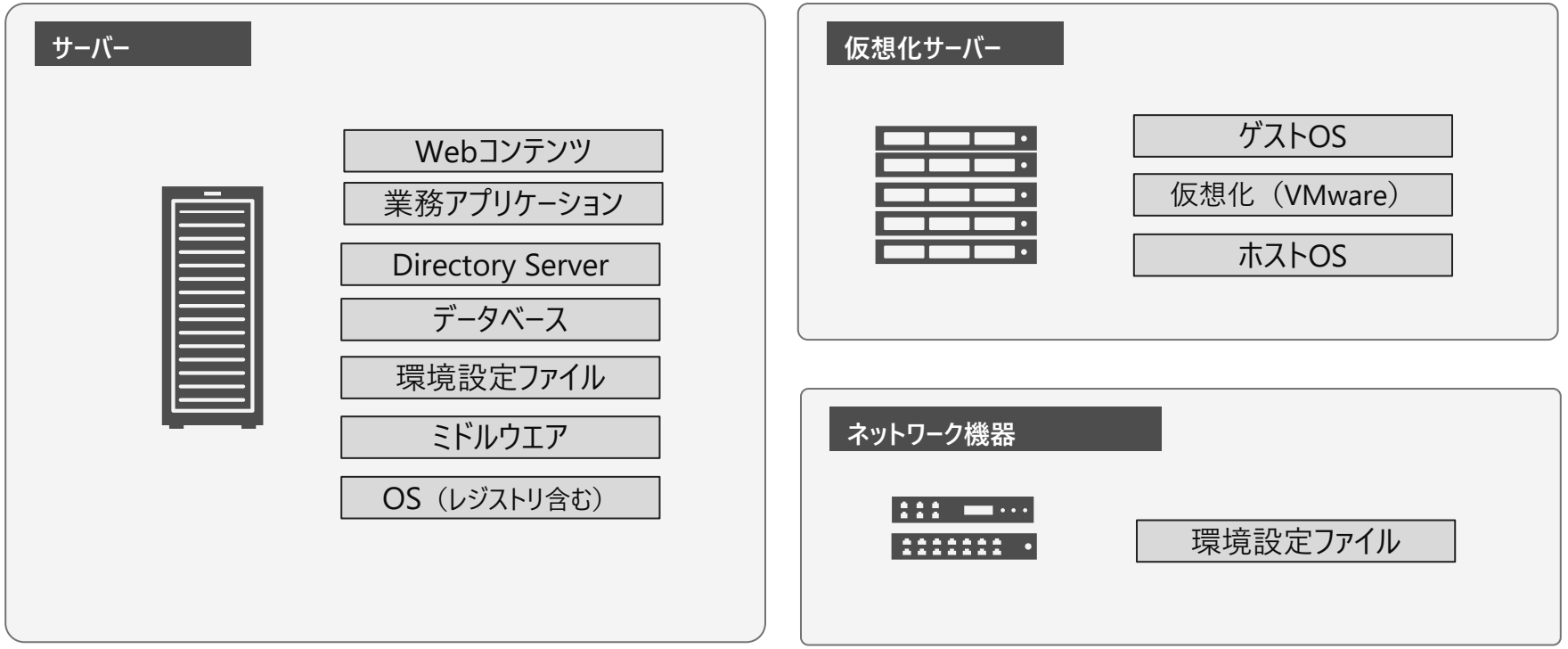
Tripwire Enterprise - 製品体系

#	製品名	製品概要
1	Tripwire Enterprise / Console（TE/Console）	サーバー機器の監視を行うにあたって必須となる製品であり、監視対象機器からの変更情報を管理
2	Tripwire Enterprise for File Systems（TE/FS）	ファイルシステム上のディレクトリ、ファイル、レジストリなど、全てのファイルを監視
3	Tripwire Enterprise for Network Devices（TE/ND）	ルーター、スイッチ、ファイアウォールなど、ネットワーク機器の構成情報の変更を監視
4	Tripwire Enterprise for Databases（TE/DB）	データベースの構成情報（ユーザー権限、テーブル、ビュー、ストアドプロシージャ）の変更を監視
5	Tripwire Enterprise for Directory Services（TE/DS）	Active Directoryのスキーマ、パスワード設定、ユーザー権限、ネットワークリソース、グループアップデートおよびセキュリティポリシーのオブジェクトや属性の変更を監視
6	Tripwire Enterprise for VMware ESX（TE/VMware）	VMware ESXサーバーが持つパラメータの変更を監視

HITACHI

Tripwire Enterprise - 監視対象項目

Tripwire Enterpriseは、システムのフォルダー、ファイルの属性（プロパティ）、レジストリ、エンドユーザー作成ファイルの属性、データベースのデータ、Directory Serverのデータなどの項目を監視できます。



プラットフォームごとのOS監視用テンプレート、PCI DSS、ISOなど各種の業界基準のテンプレートを**Fortra社が無償で提供**

HITACHI

Tripwire Enterprise - 主な製品対応OS（Manager）

Tripwire Enterprise / Server
Windows Server 2016 (x86_64)
Windows Server 2019 (x86_64)
Windows Server 2022 (x86_64)
Windows Server 2025 (x86_64)
Red Hat Enterprise Linux 8.0 - 8.10 (x86_64)
Red Hat Enterprise Linux 9.0 - 9.5 (x86_64)

バックエンド データベース
Oracle 19c
MySQL 8.0.x

Webコンソール サポート対象Webブラウザー
Microsoft Edge バージョン90以降
Google Chrome バージョン90以降
Mozilla Firefox バージョン68以降

Tripwire Enterprise - 主な製品対応OS（Agent）

Tripwire Enterprise / FS
Windows 10, 11 (x86_64)
Windows Server 2016, 2019, 2022, 2025 (x86_64)
Red Hat Enterprise Linux 8.0 - 8.10, 9.0 - 9.5 (x86_64)
Oracle Linux 8.0 - 8.9, 9.0 - 9.3 (x86_64)
Oracle Solaris 11.4 (x86_64, SPARCv9)
IBM AIX 7.2 (Power7, Power8, Power9) , 7.3 (Power9, Power10)

Tripwire Enterprise / DB
IBM DB2 11
MariaDB Server 10.11
SQL Server 2016, 2017, 2019, 2022
Oracle 19c
PostgreSQL 13, 14, 15, 16

Tripwire Enterprise / VE
VMware vSphere 7.0

Tripwire Enterprise / DS
Microsoft Active Directory
（サポートされるディレクトリサービス製品は、別途お問い合わせください。）

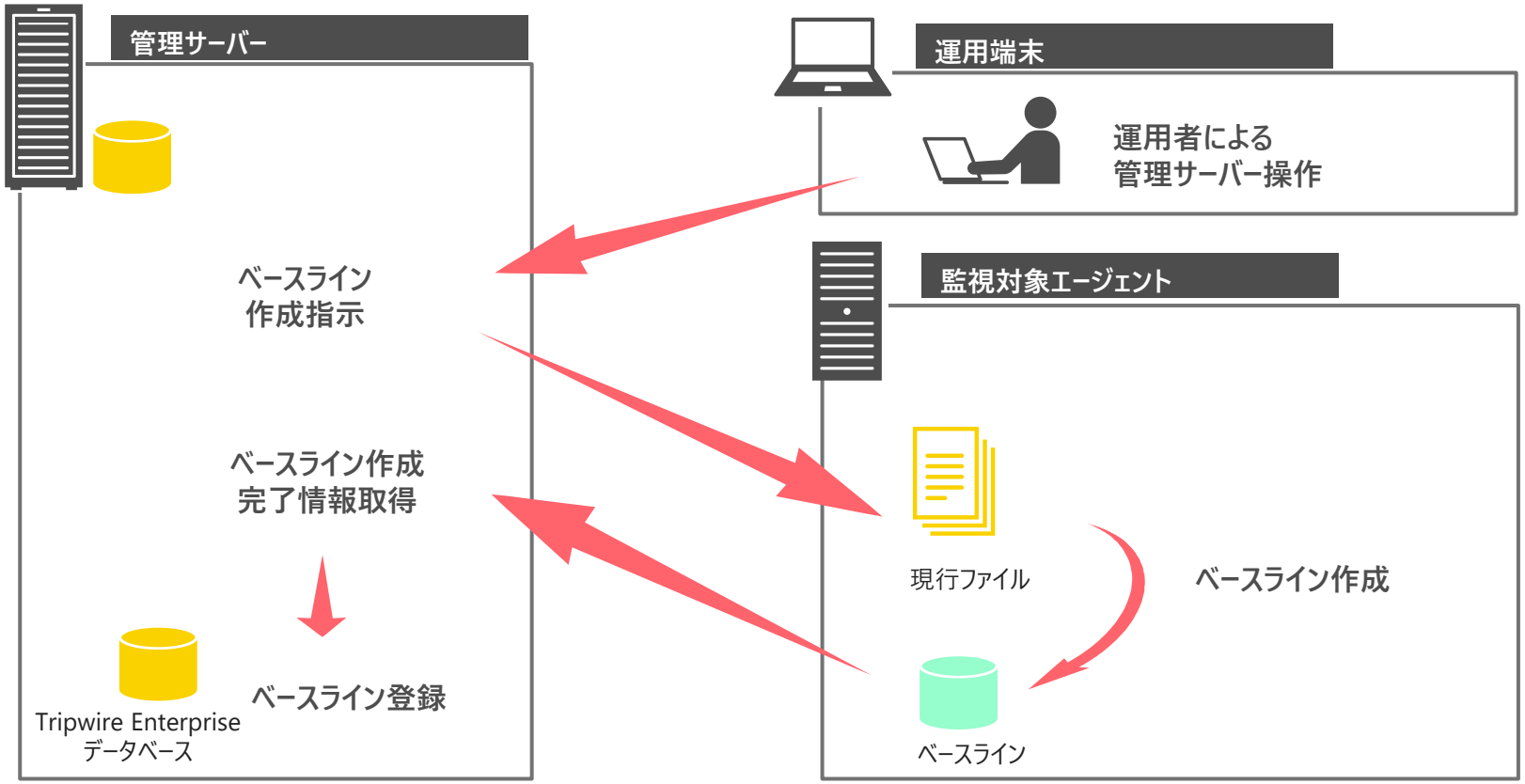
以下、Fortra社Webサイトより抜粋。最終更新日2025年5月15日時点の情報です。最新情報は、当社にお問い合わせください。
https://www.tripwire.com/legal/support-maintenance/policy/tripwire-platform-support

4. Tripwire Enterprise製品機能

HITACHI

製品機能 - ベースライン作成機能

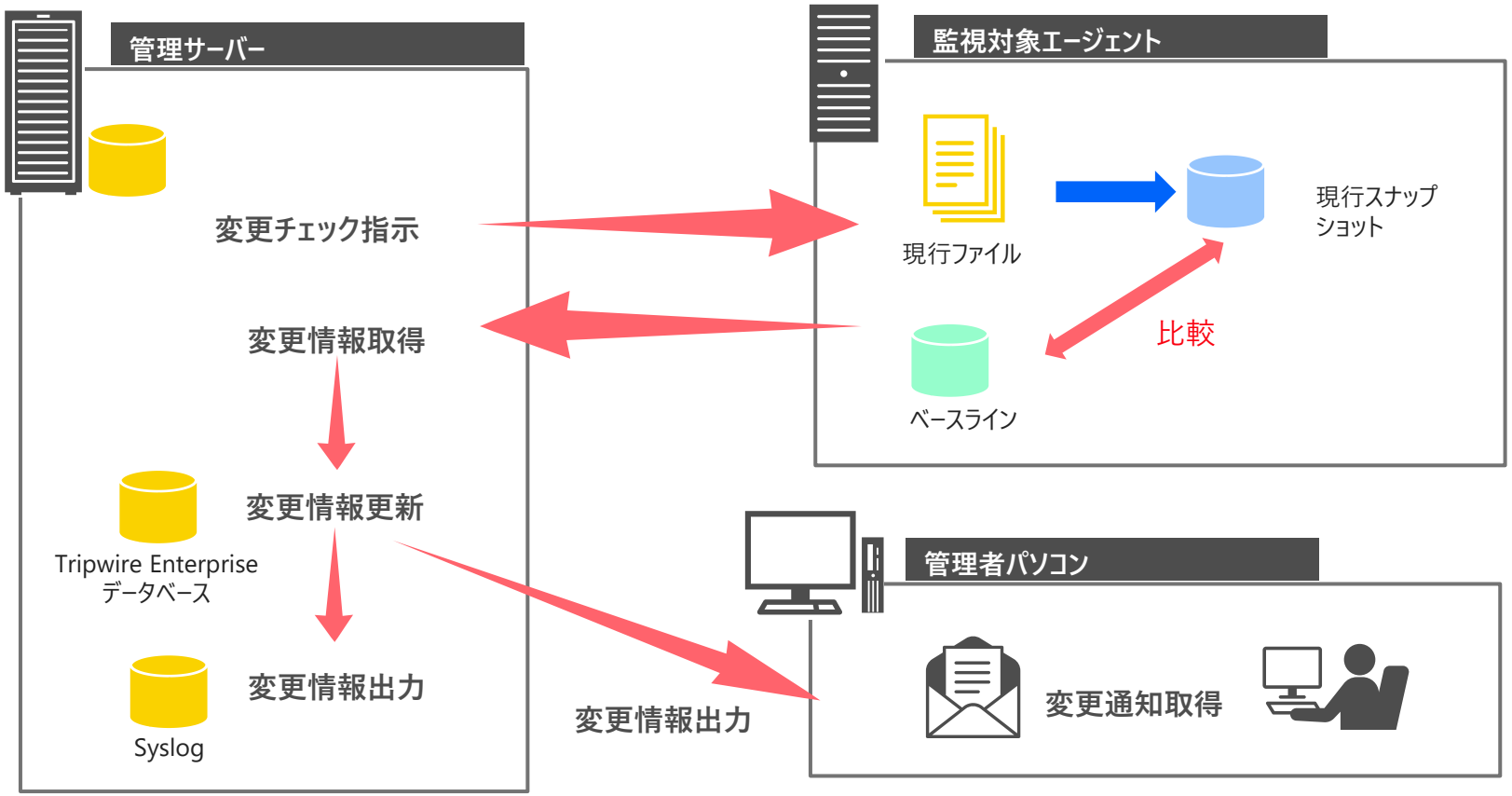
- 運用者は管理サーバーより監視対象エージェントに対してベースライン作成指示を行う
- 監視対象エージェントはベースラインを作成し、管理サーバーへ結果を返す
- 管理サーバーはベースラインをデータベースに登録する



HITACHI

製品機能 - 変更チェック機能

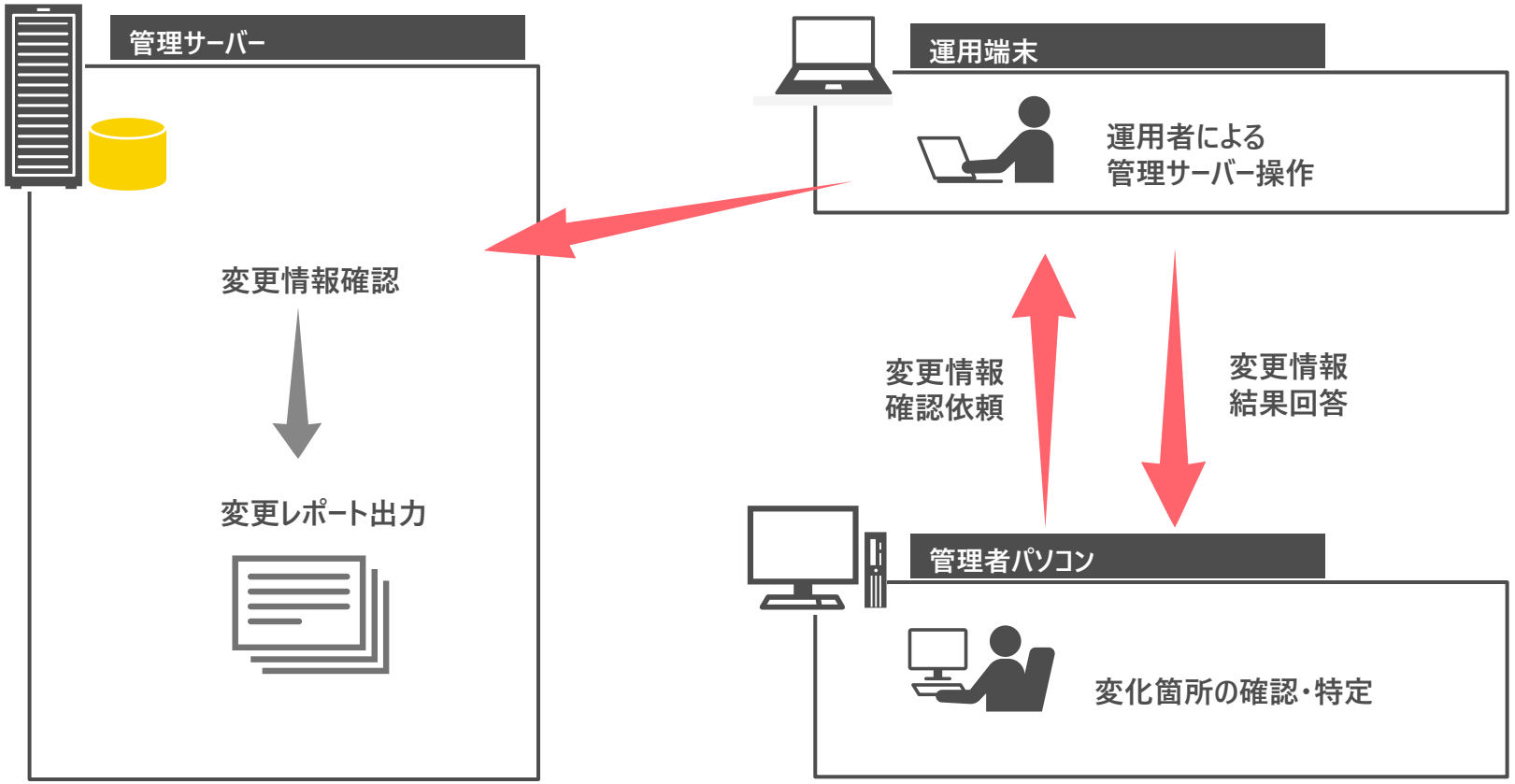
- 管理サーバーより定められた日時に監視対象エージェントに対して変更チェック指示を行う
- 監視対象エージェントは変更チェックを行い、比較結果を管理サーバーへ返す
- 管理サーバーは変更情報を更新し、定義されたメールアドレスに対して変更結果を送信し変更情報をSyslogに出力



HITACHI

製品機能 - 変更情報確認機能

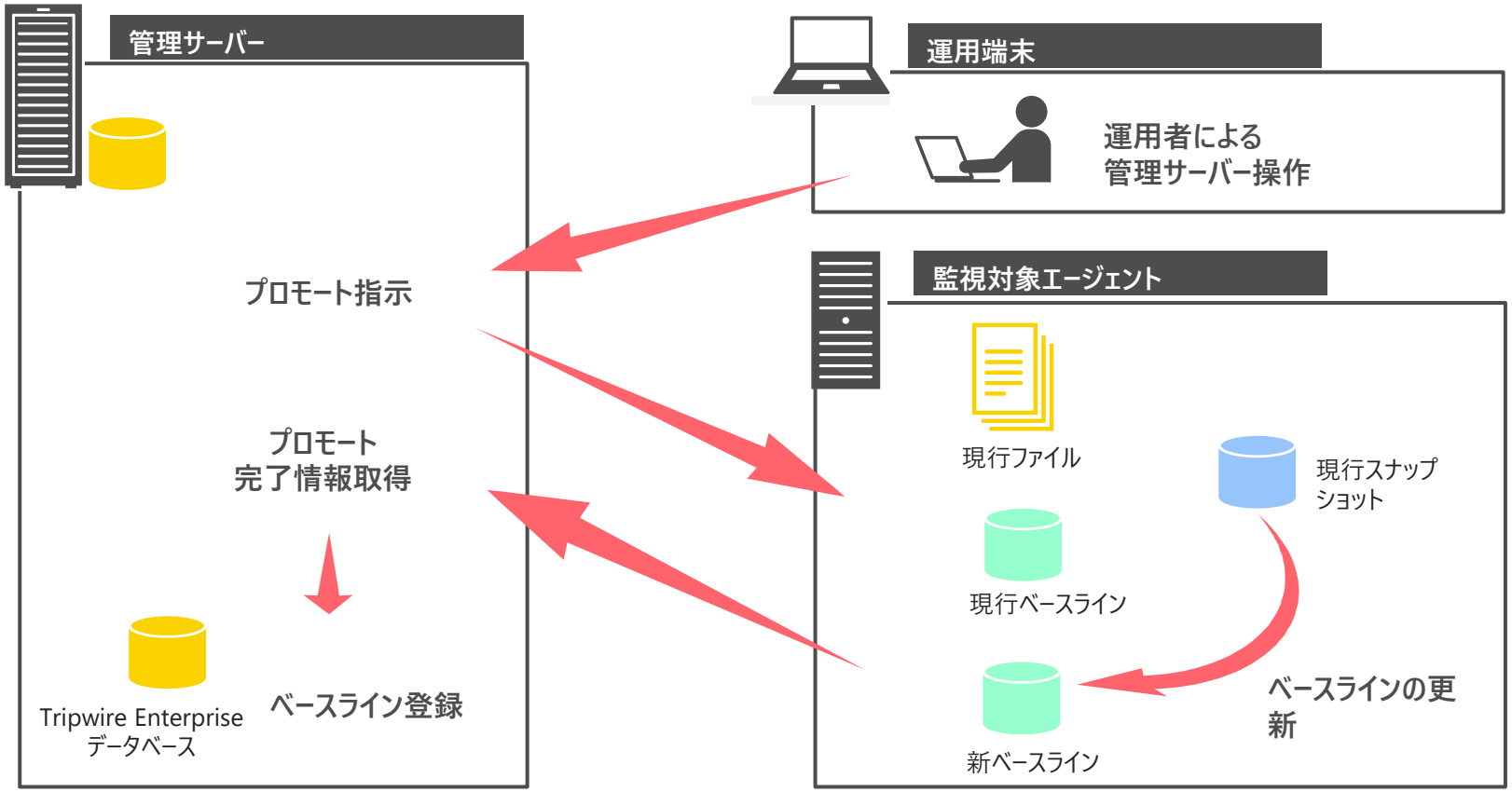
- 管理者からの変更情報確認依頼に対して運用者は管理サーバーから確認情報を取得する
- 運用者は必要に応じて変更レポートを作成する
- 運用者は管理者に対して変更情報確認結果を回答する



HITACHI

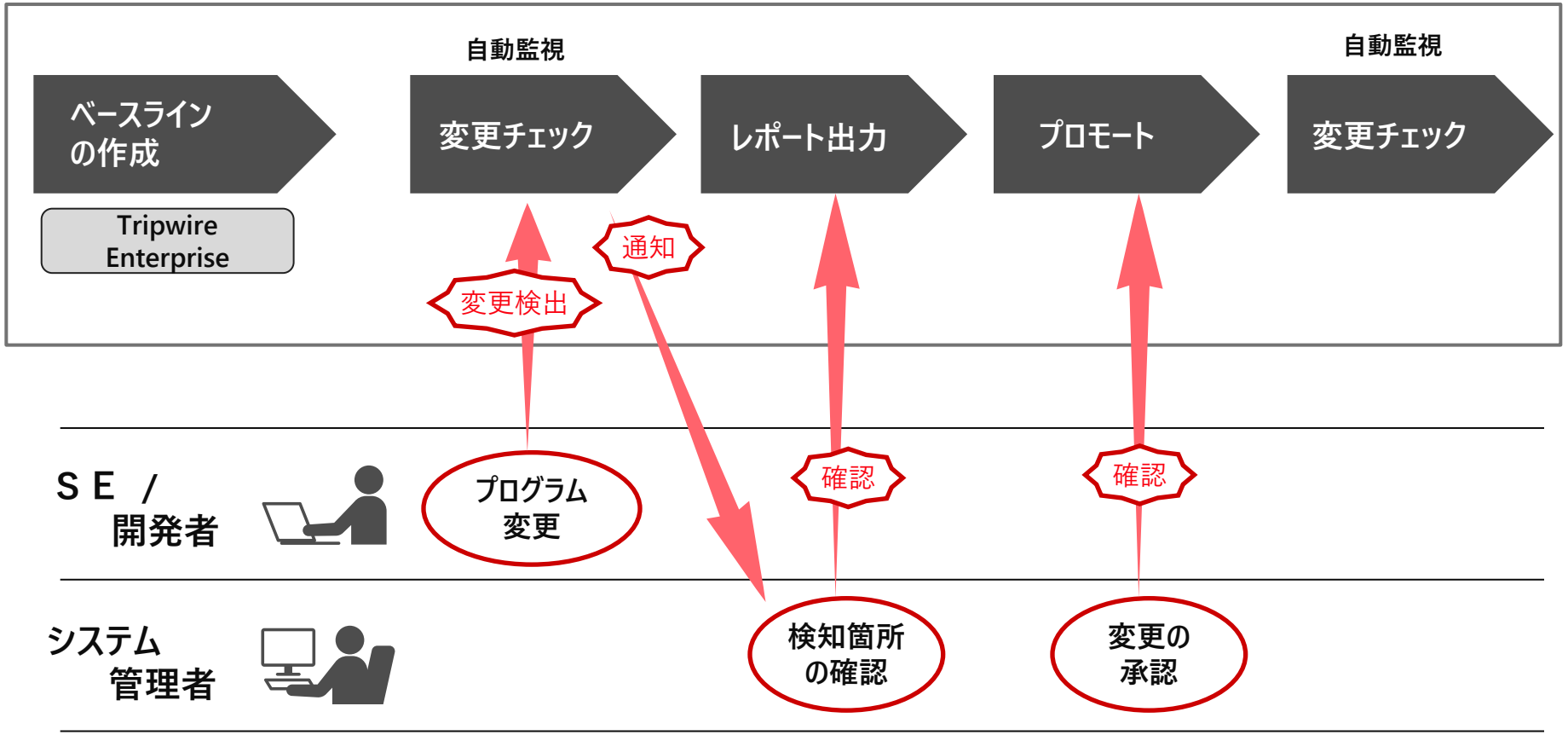
製品機能 - プロモート（ベースライン更新）機能

- 運用者は管理サーバーから監視対象エージェントに対してプロモート指示を行う
- 監視対象エージェントは新ベースラインを作成し、管理サーバーへ結果を返す
- 管理サーバーは新ベースラインをデータベースに登録する



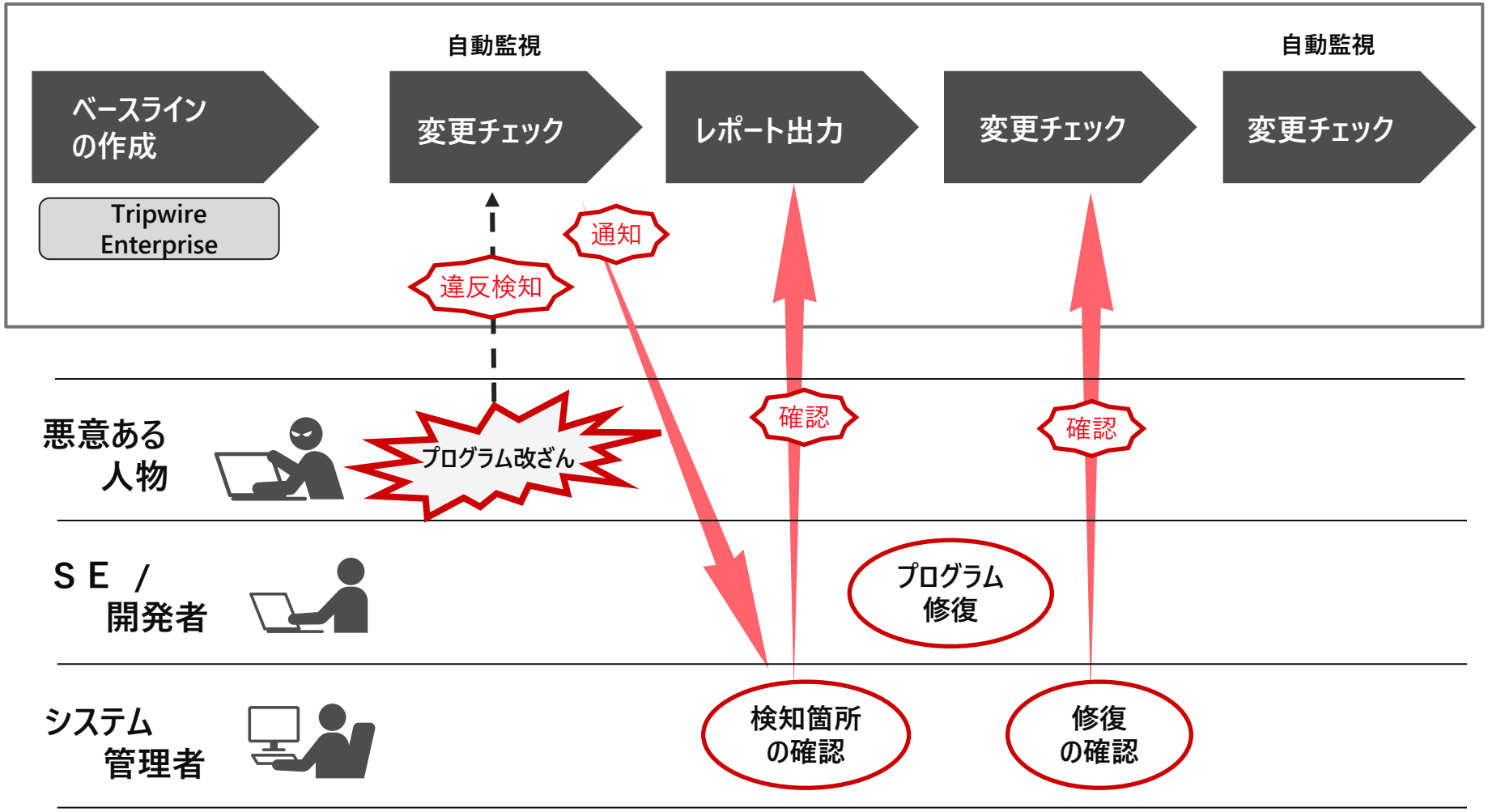
HITACHI

■プログラム変更時の運用例



HITACHI

■改ざん時の運用例



5. Fortra社について

HITACHI

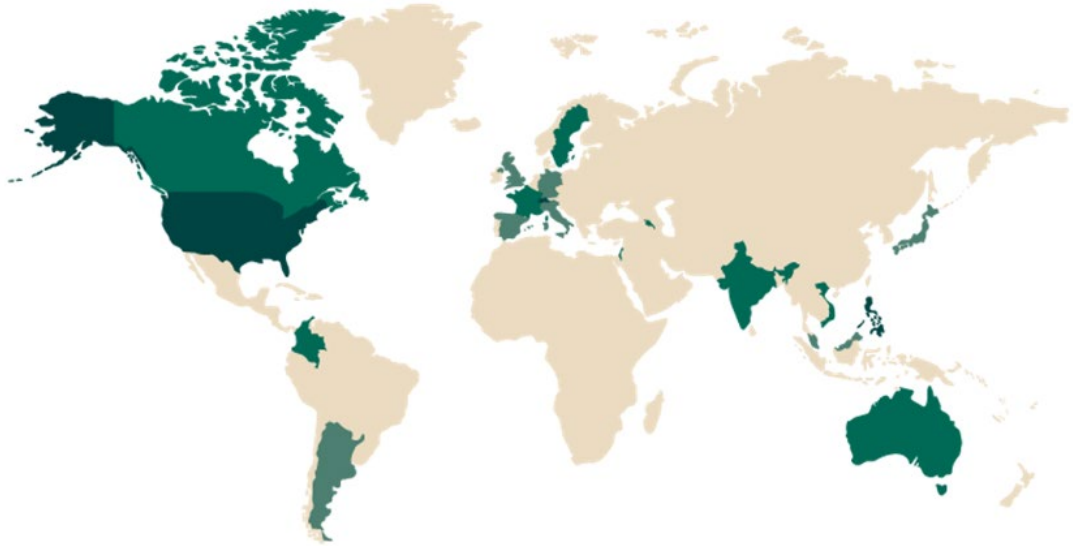
■Fortra社 会社概要

売上額：8億ドル以上

現地法人数：18

社員数：3,000人以上

累計顧客数：約30,000社以上
（世界91カ国）



FORTRA™

6. 日立ソリューションズ・クリエイトのソリューション

HITACHI

日立ソリューションズ・クリエイトはTripwire認定資格３種類を保持しています

Tripwireゴールドリセラー

【取得資格】

- Certified Consultant　コンサルタント認定資格
- Certified Professional　機能プロフェッショナル認定資格
- Certified Operator　機能操作認定資格

国内初
2017年に取得済

豊富な大型案件の導入実績

Tripwire Enterprise	導入事例	◆ 某金融機関　（監視対象：250台） [用途]　Web改ざん対策、PCI DSS対応
		◆ 某公共機関　（監視対象：100台） [用途]　IT統制

導入支援実績（2024年11月時点）

業界	件数
社会・公共	14
メーカー	13
金融	12
サービスなど（旅行・小売）	8
合計	47

さまざまな業界・規模のお客さまの要件に合わせた
導入支援を行ってきました

ソリューション活用例

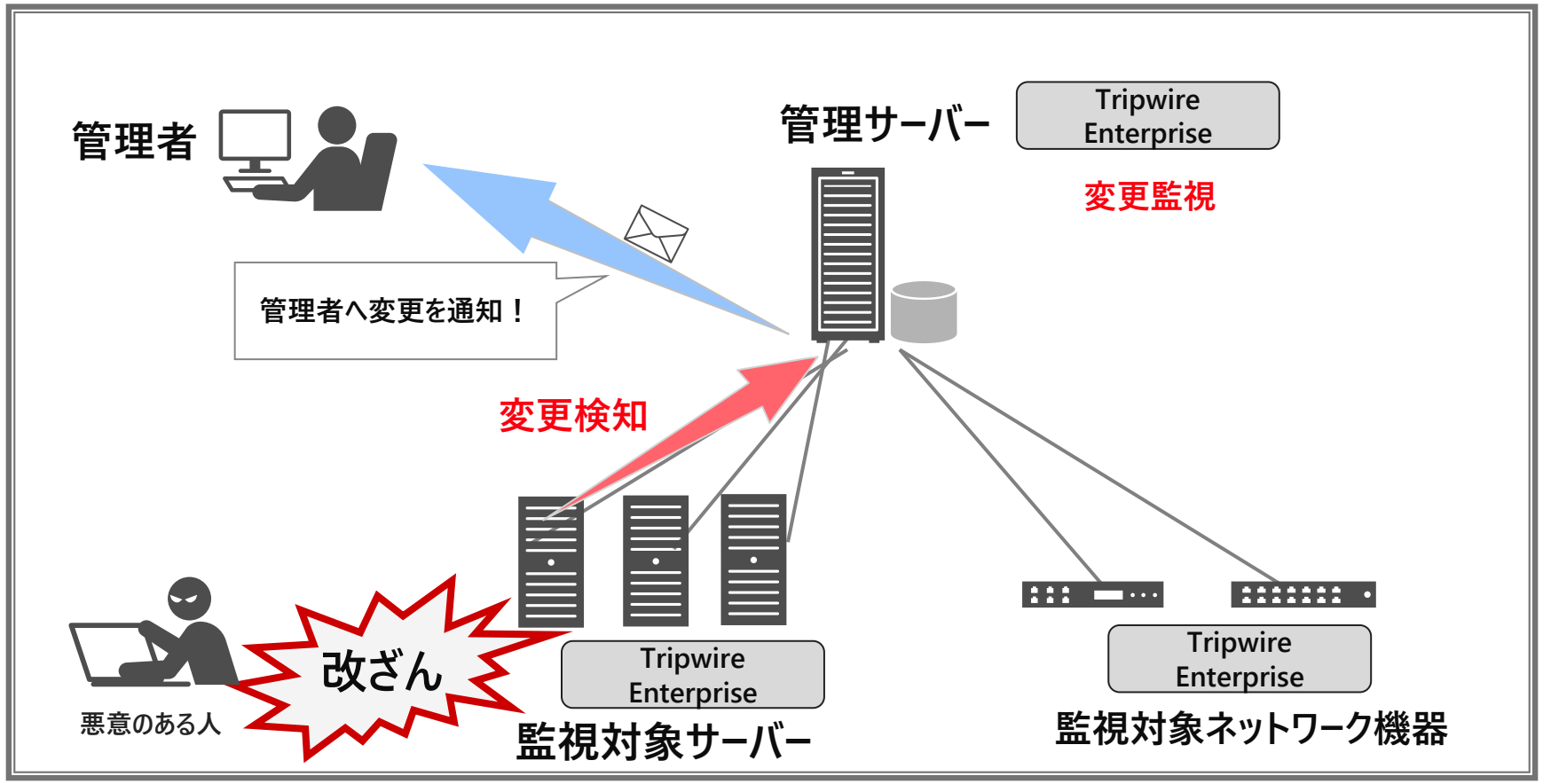
【要件】
- ✓ 変更検知の仕組み導入したい
- ✓ PCI DSS、J-SOXなどのIT全般統制への対応を強化したい
- ✓ 変更状況の可視化（いつ、誰が、どのような変更を実施したか）
- ✓ 未承認の更新情報の洗い出し
- ✓ Webコンテンツの変更検知　など

【必要な作業】
- ✓ 監視対象サーバーや変更監視対象の選定
- ✓ 監視設計および監視ルール確定、運用方針の決定
- ✓ 製品の導入および監視ルールや監視条件の設定
- ✓ 動作確認テスト

HITACHI

Security Web改ざん検知システム

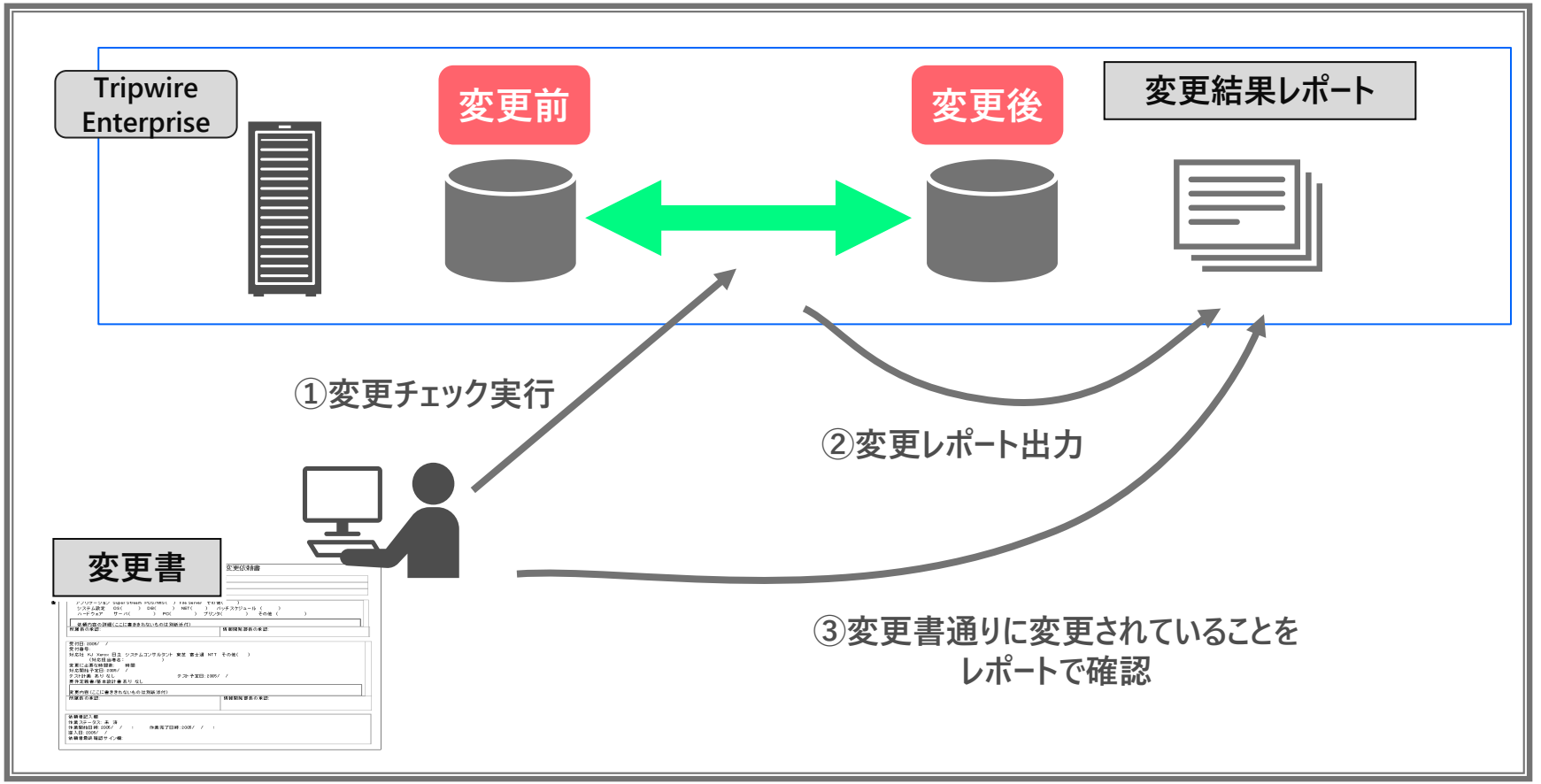
既知の変更、未知の変更（改ざん）されたファイル名を正確に検知・通知します。



HITACHI

Availability システム変更チェックシステム

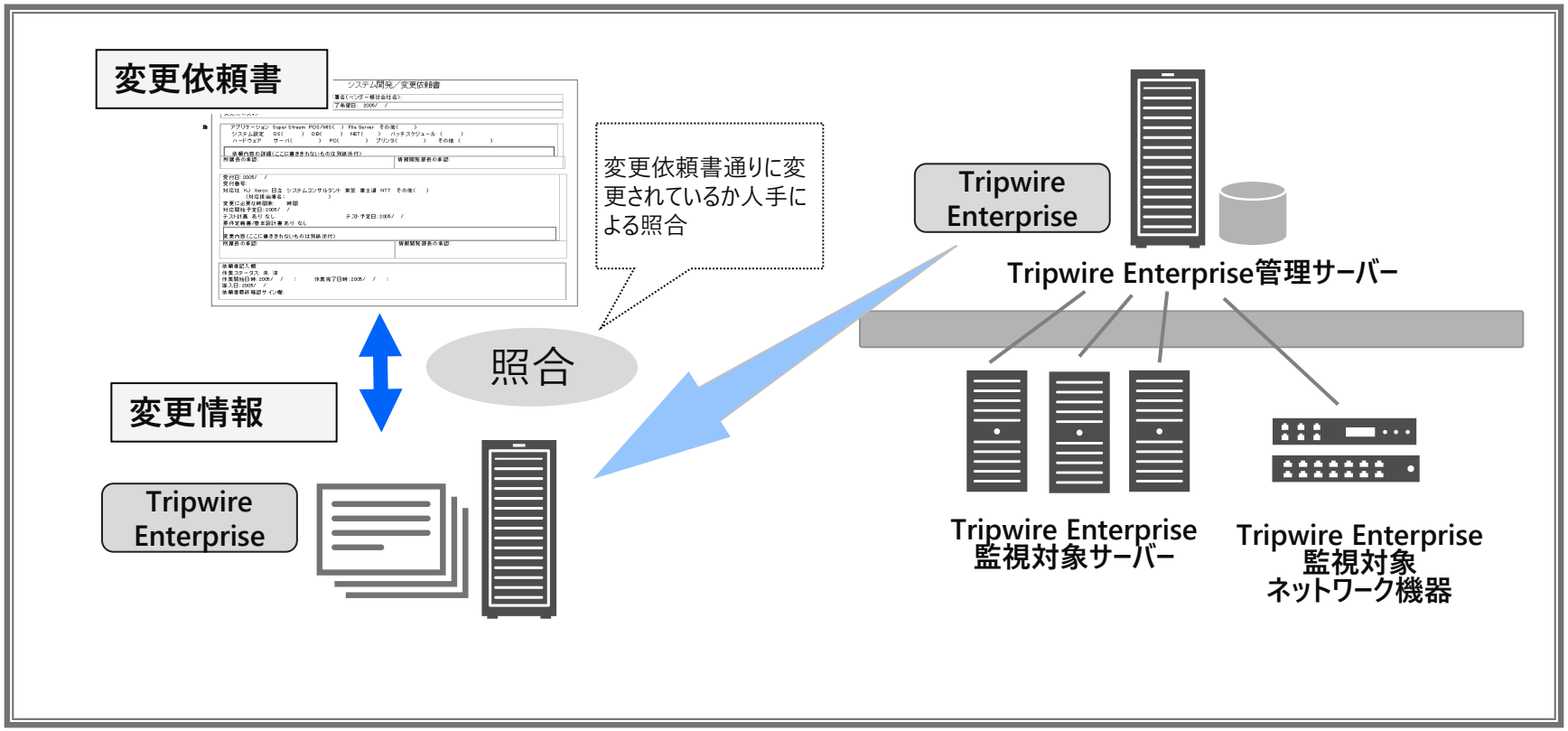
意図した変更が的確に実施されたか、結果レポートで確認します。



HITACHI

Compliance 変更管理システム

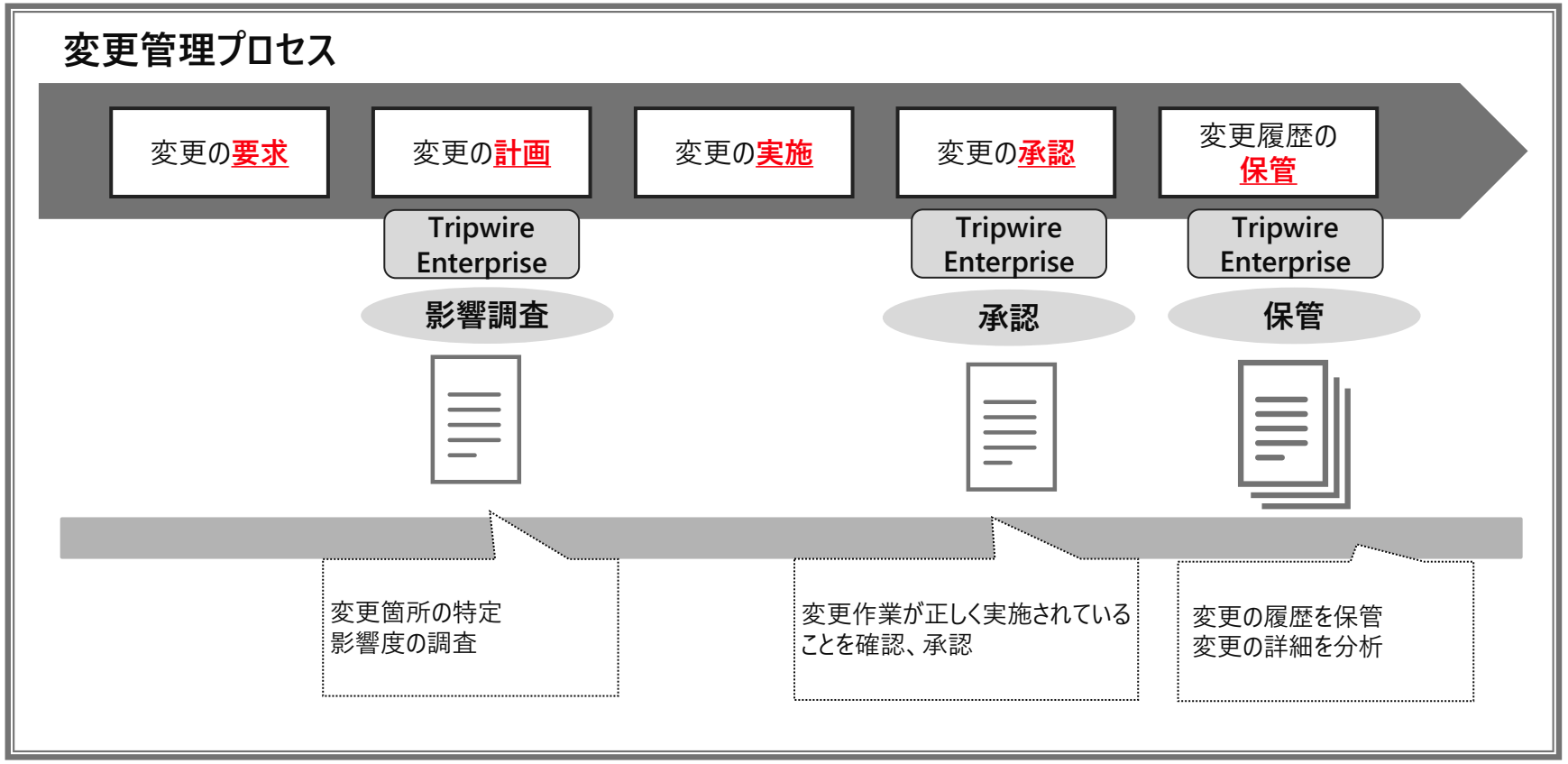
意図した変更作業が的確に実施されたか、システム管理者が変更依頼書と結果レポートで照合確認します。
結果レポートは変更の監査証跡として内部・外部監査時に利用できます。



HITACHI

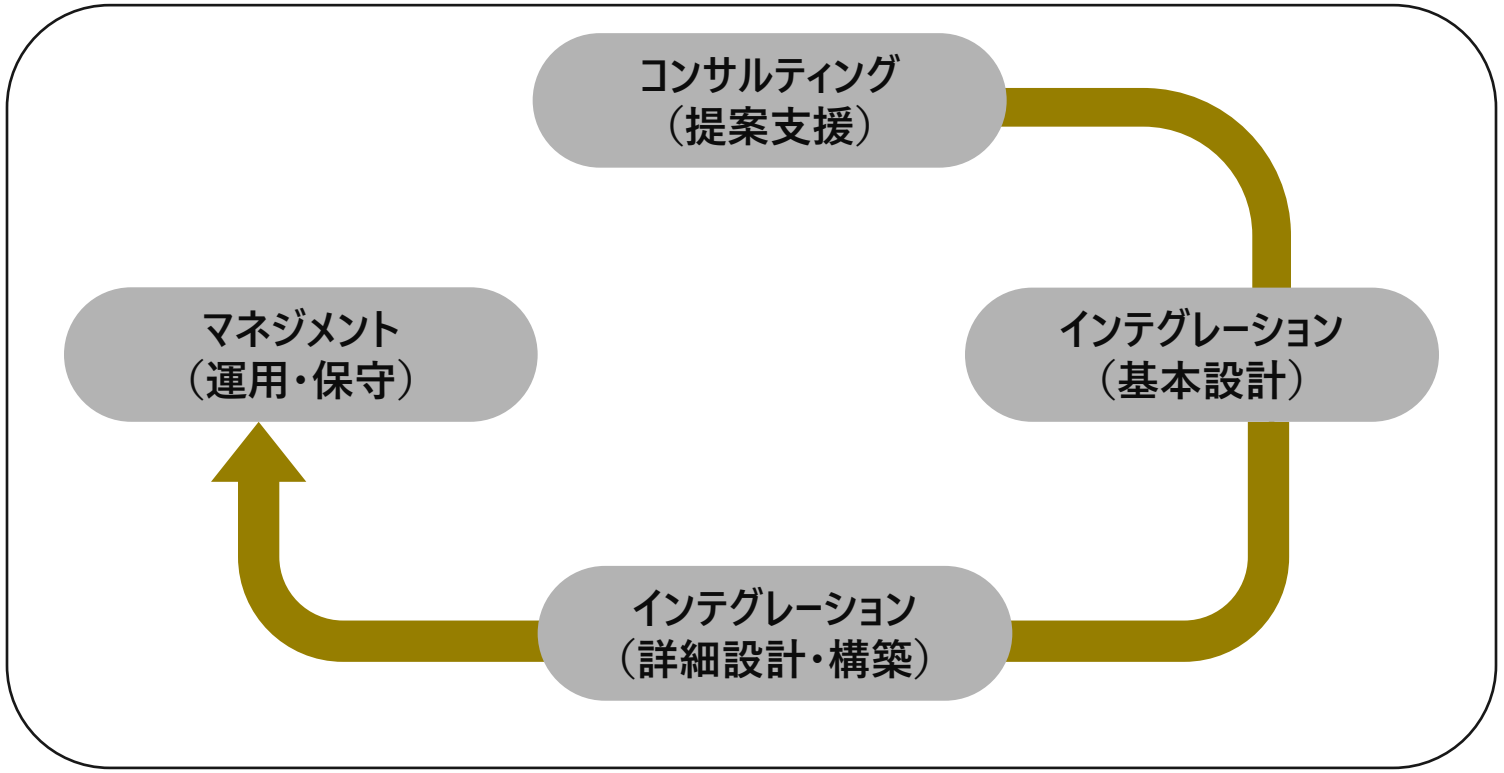
Compliance 変更管理システム

変更管理プロセスに係る運用業務に必要とされる、変更の計画／承認／変更履歴の保管を効率的に支援します。



ソリューションサービスの特長

当社のソリューションサービスは、コンサルティングからシステムの設計・
構築・運用・保守までの各種ソリューションを提供します。
Tripwire Enterpriseの特長であるシステムの変更管理運用を効率的に行います。



ソリューションサービスのメニュー

コンサルティングからシステムの設計・構築・運用・保守まで、
システム全体をカバーしたサービス群を提供します。

フェーズ	サービス商品名	内容
コンサルティング	提案支援サービス	製品の紹介、提案書作成支援、デモを実施します。 導入を検討しているお客さまへの提案支援を行います。
	要件整理支援サービス	製品適用に関する現行環境構成確認、要件定義書作成、 スケジュール確定などの導入要件整理を行います。
インテグレーション （基本設計）	設計支援サービス	ご要件に沿った基本設計・運用設計を行います。
インテグレーション （詳細設計・構築）	導入支援サービス	Tripwire Enterpriseのインストール、設計支援サービスに基づいた 詳細設計、環境設定、テストを実施します。
	インストレーションサービス	Tripwire Enterpriseのインストール、弊社規定の設定シートに従った 簡易設定、製品の動作確認まで行います。
マネジメント （運用・保守）	操作教育サービス	Tripwire Enterpriseに関する運用・保守の操作教育の支援をします。
	ルール変更支援サービス	本番稼働後の変更検知箇所の変更、追加、削除などの 環境再設定の支援を行います。

お問い合わせ先

HITACHI

■お問い合わせ先

株式会社 日立ソリューションズ・クリエイト

- **Webでのお問い合わせ**
  www.hitachi-solutions-create.co.jp/contact/solution.html

  お問い合わせページより、商品・サービスをお選びください。
- **メールでのお問い合わせ**
  hsc-contact@mlc.hitachi-solutions.com

■お問い合わせ情報について

ご相談、ご依頼いただいた内容は回答などのため、当社の関連会社（日立ソリューションズグループ会社）および株式会社日立製作所に提供（共同利用含む）することがあります。
取り扱いには充分注意し、お客さまの許可なく他の目的に使用することはありません。

表示に関する注意事項

HITACHI

■他社商品名、商標などの引用に関する表示

- Tripwireは、Fortra Inc.の登録商標です。
- American Expressは、American Express Marketing & Development Corp.の登録商標です。
- DISCOVERは、Discover Financial Services LLCの登録商標です。
- JCBは、株式会社ジェーシービーの登録商標です。
- MasterCardは、Mastercard International Incorporatedの登録商標です。
- VISAは、Visa International Service Associationの登録商標です。
- Windows、Microsoft Edge、SQL Serverは、米国、その他の国における米国Microsoft Corp.の登録商標です。
- Linuxは、Linus Torvaldsの米国およびその他の国における登録商標あるいは商標です。
- Oracle、MySQLは、Oracle Corporationの登録商標です。
- Firefoxは、Mozilla Foundationの米国およびその他の国における商標または登録商標です。
- Chromeは、Google LLCの登録商標です。
- CentOS、Red Hat Enterprise Virtualizationは Red Hat, Inc.の登録商標です。
- AIX、DB2は、IBM Corporationの登録商標です。
- HP-UXは、Hewlett-Packard Development Company, L.P.の登録商標です。
- PostgreSQL は、The PostgreSQL Global Development Groupの商標です。
- VMwareは、VMware, Inc.の登録商標です。

表示に関する注意事項

HITACHI

- Ciscoは Cisco Systems, Inc. の登録商標です。
- Extremeware SwitchesはExtreme Networks, Inc.の登録商標です。
- F5 BIG-IPはF5 Networks, Inc.の登録商標です。
- Juniper M&T、Juniper NetscreenはJuniper Networks, Inc.の登録商標です。
- Nortel AlteonはRadware、Nortel PassportとNortel Web OSはAvayaの登録商標です。

■サービス・製品の仕様に対する表示

本資料に記載しているサービス・製品の仕様は、2025年11月現在のものです。
サービス・製品の改良などにより予告なく記載されている仕様が変更になることがあります。


HITACHI