

---

## Tripwire Enterpriseのご紹介



株式会社 日立ソリューションズ・クリエイト

# Contents

---

1. Tripwire Enterpriseのご紹介
2. Tripwire Enterprise活用イメージ
3. Tripwire 製品概要
4. Tripwire 製品機能
5. Tripwire社について
6. 日立ソリューションズ・クリエイトについて

## ■ Tripwire Enterprise とは

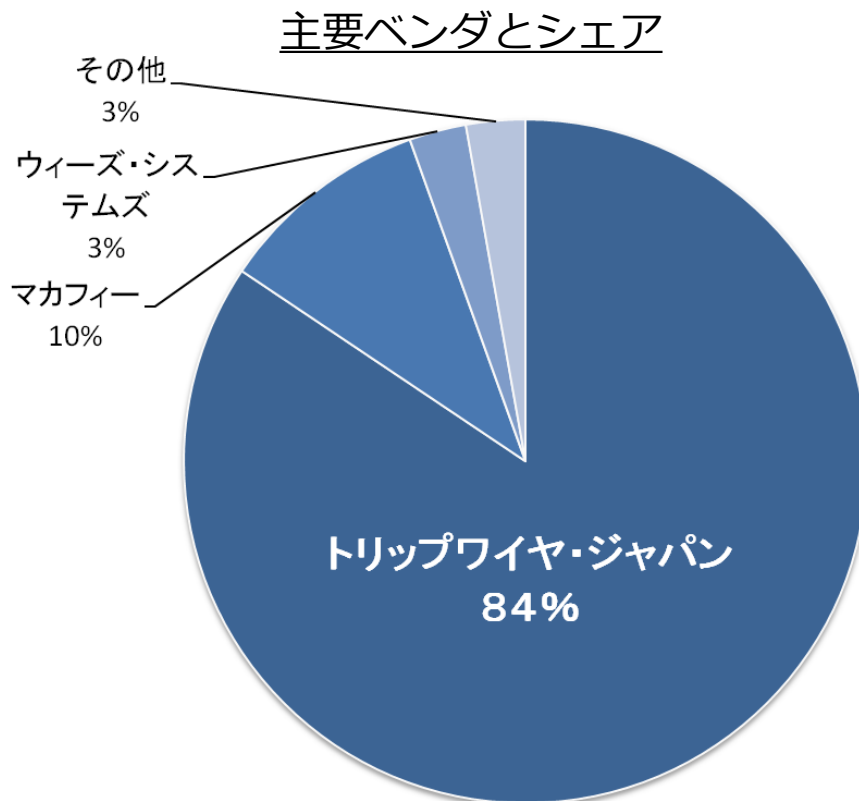
Tripwireは、「変更コントロールソフトウェア」で、サーバ、クライアント、ネットワーク機器などのITインフラに加えられる変更を一元的に、且つ、常に監視・管理するソフトウェアパッケージです。



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

マーケットシェアNo.1



出典 株式会社ミック経済研究所  
「情報セキュリティソリューション市場の現状と将来の展望 2014年度版」

## 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3要素を構成する「整合性」を維持します。ITシステムの整合性監視によって、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**3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あらゆる変更を検知することでセキュリティの強化、可用性の向上と真正性の証明を実現します。



## Tripwire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

## Tripwire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

1997年にTripwire, Inc. が米オレゴン州ポートランドに設立され、変更検知に特化した商用ソフトウェアの開発、販売を開始し、現在では9,000社以上の導入実績を持ちます。

Tripwire Enterprise は、日本においても主に官公庁、金融業界を中心に1,000社近くの導入実績を誇っています。

経済産業省の情報処理推進機構 (IPA)において、改ざん検知のソフトウェアとして Tripwire for Servers、および後継製品として 2005年に発売された Tripwire Enterprise の採用が推奨されています。

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遵守のために Tripwire 製品の使用が事実上必須となりました。

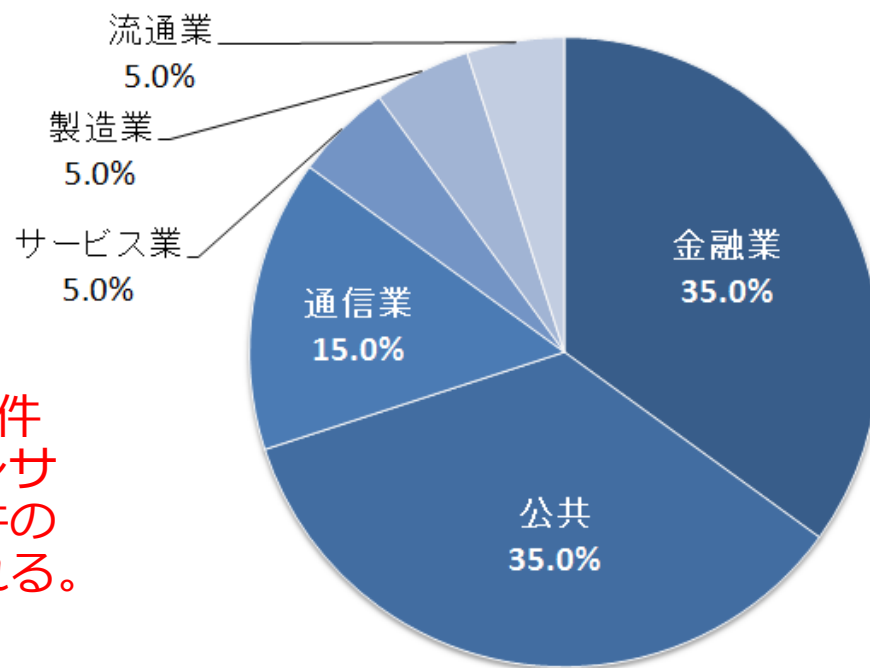
PCI DSSのVer1.0には、要件11.5のファイル完全性監視ソフトウェアとして “Tripwire” と具体的な製品名が明記されています。

## ■ Tripwire Enterprise 導入先

Tripwire Enterpriseの導入は、大規模企業、且つ、コンプライアンスに厳格な金融業界、大手テレコム業界、官公庁が進んでいる。

他に、変更コントロールという観点で、コンプライアンス、ITサービスの継続性が該当することから、ITサービスの継続性を重視する大手企業では導入されている。

業種別販売ウエイト



今後の市場は、PCIDSSに関連した案件やサイバー攻撃の増加に伴って、コンサルティングを行いながら提案する案件の増加が好調に推移することが予想される。

出典 株式会社ミック経済研究所  
「情報セキュリティソリューション市場の現状と将来の展望 2014年度版」

# Contents

---

1. Tripwire Enterpriseのご紹介
- 2. Tripwire Enterprise活用イメージ**
3. Tripwire 製品概要
4. Tripwire 製品機能
5. Tripwire社について
6. 日立ソリューションズ・クリエイトについて

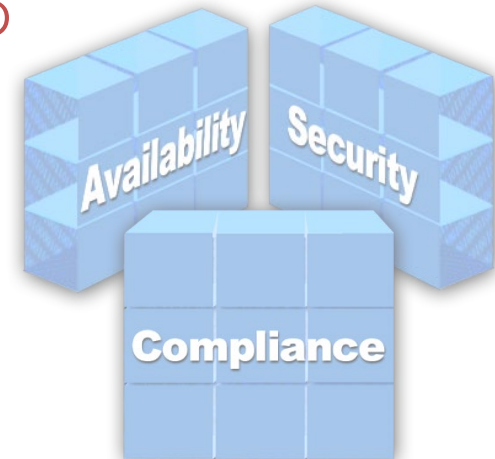


### Security

## データの改ざんを検知

セキュリティ対策には 100 % 確実なものはありません。  
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, サーバやネットワーク機器のあらゆる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」**を通知することができます。

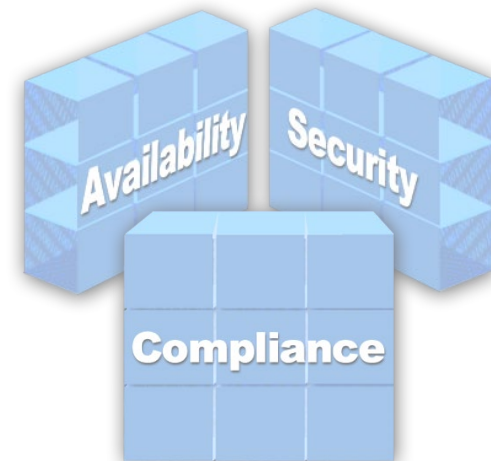


### Availability

## 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することが可能です。抜け穴のない**変更管理プロセス遵守を徹底**することができます。

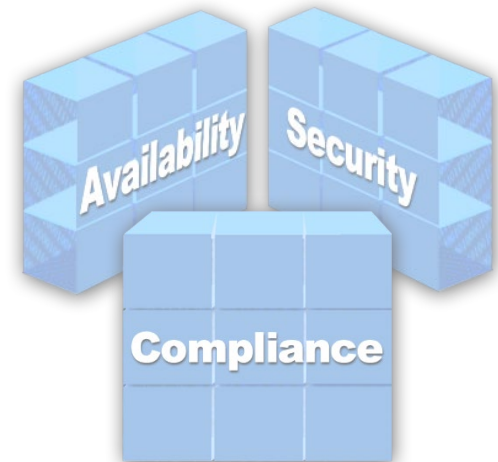


### Compliance

## 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。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でき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することができます。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。



# Contents

---

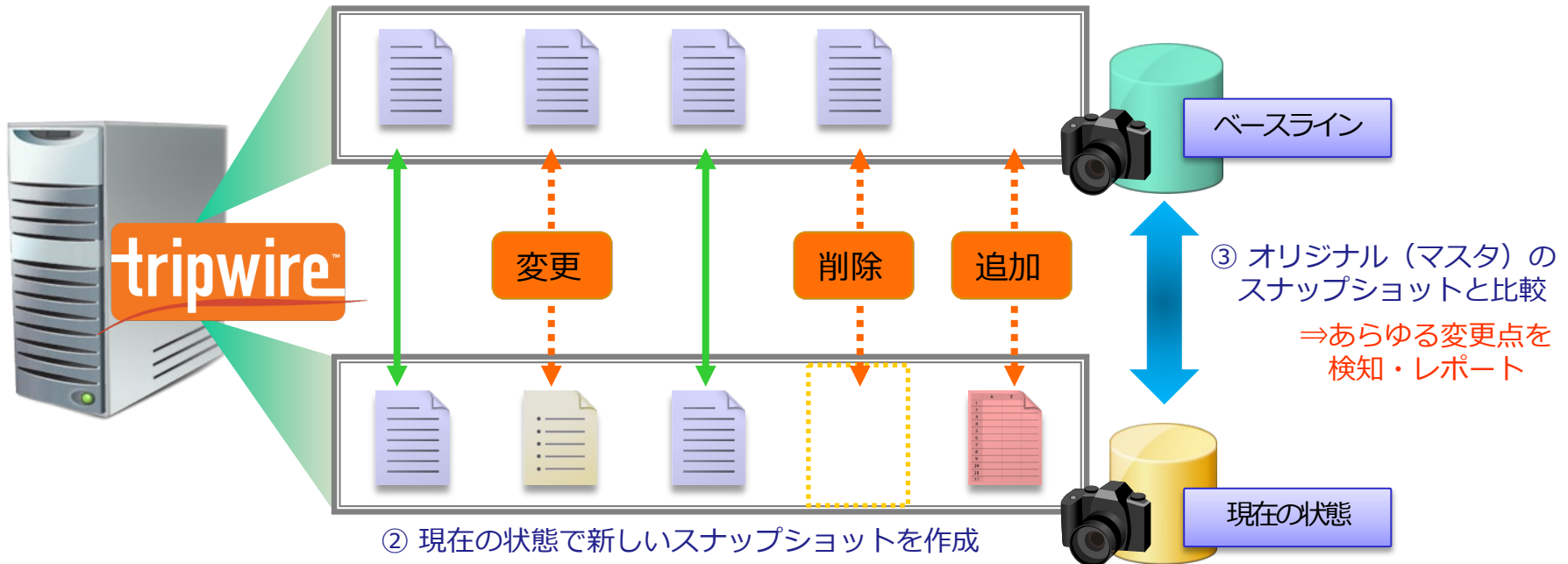
1. Tripwire Enterpriseのご紹介
2. Tripwire Enterprise活用イメージ
- 3. Tripwire 製品概要**
4. Tripwire 製品機能
5. Tripwire社について
6. 日立ソリューションズ・クリエイトについて

## Tripwire Enterprise - コアテクノロジー



Tripwire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 システムの正しい状態のときにデータのデジタルスナップショット（ベースライン）を作成



② 現在の状態で新しいスナップショットを作成

※1：最適な状態のデジタルスナップショット

## Tripwire Enterprise - 製品体系



### 管理サーバ

Tripwire Enterprise / Server



バックエンドDB  
( Oracle, MySQL )

### 管理PC

Web browser  
( Internet Explorer , Firefox )



### 監視対象エージェント



Tripwire Enterprise / FS  
【Server,PC】



Tripwire Enterprise / DB  
【Database】



Tripwire Enterprise / DS  
【Directory Server】



Tripwire Enterprise / VMWare ESX  
【 VMWare 】



Tripwire Enterprise / ND  
【 Network Device 】



Tripwire Enterprise / POS  
【 POS Server,POS 】

## Tripwire Enterprise - 監視対象項目

Tripwireは、システムのフォルダ、ファイルの属性（プロパティ）、レジストリ、エンドユーザ作成ファイルの属性、DataBaseのデータ、DirectoryServerのデータなどの項目を監視できます。

### サーバ



- Webコンテンツ
- 業務アプリケーション
- Directory Server
- Data Base
- 環境設定ファイル
- ミドルウェア
- OS (レジストリ含)



### 仮想化サーバ



- ゲストOS
- 仮想化 (VMWare)
- ホストOS

### ネットワーク機器



- 環境設定ファイル

プラットフォームごとのOS監視用テンプレート、PCIDSS、ISOなどの各種の業界基準のテンプレートを[トリップワイヤ社が無償で提供](#)

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

### Tripwire Enterprise / Server

Windows Server 2012 (x86\_64)  
Windows Server 2012 R2 (x86\_64)  
Windows Server 2016 (x86\_64)  
Windows Server 2019 (2004,20H2) (x86\_64)  
Red Hat Enterprise Linux 7.0 - 7.9 (x86\_64)  
Red Hat Enterprise Linux 8.0 - 8.5 (x86\_64)  
CentOS 8.4 - 8.5 (x86\_64)  
Oracle Linux RHCK 7.9, 8.0 - 8.5 (x86\_64)

※ Tripwire Enterprise 8.4から64bitOSのみの対応となっております。

### バックエンド データベース

SQL Server 2008 SP4, 2008 R2 SP2, 2012, 2014, 2016, 2017, 2019  
Oracle 11g R2 (11.2.0.1 - 11.2.0.3), 12c R1,1 8c, 19c  
Oracle RAC 11g R2, 12c  
MySQL 8.0.x  
MariaDB 10.4  
Amazon Aurora (MySQL 5.7-compatible)

### Webコンソール サポートブラウザ

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 7, 8, 8.1, 10(10,1909,2004,20H2), 11 (x86\_64)  
Windows Server 2012,2012 R2, 2016, 2019(2004,20H2) (x86\_64)  
Red Hat Enterprise Linux 7.0 - 7.9, 8.0 - 8.5 (x86\_64)  
CentOS 7.0 - 7.9, 8.0 - 8.5 (x86\_64)  
Oracle Linux RHCK 7.2 - 7.9, 8.0 - 8.5 (x86\_64)  
Oracle Solaris 11.0 - 11.4 (x86\_64, SPARCv9)  
IBM AIX 7.1 (64 bit, Power 6,7,8) , 7.2 (64 bit, Power 8)  
HP-UX 11i v3 UD7-UD9 (Itanium)  
Mac OS X 10.8.2 - 10.8.5 (x86\_64)  
Amazon Linux 2015.09 (4.1.10-17.31), (4.1.13-19.31), (4.1.17-22.30) (x86\_64)

### Tripwire Enterprise / VE

VMware ESXi 5.0, 5.1, 5.1 U1, 5.5, 6.0, 6.5, 6.7, 7.0  
VMware vSphere 5.0, 5.1, 5.1 U1, 5.5, 6.0, 6.5, 6.7, 7.0  
Red Hat Enterprise Virtualization Guest 6.0 2.6.32-71  
Red Hat Enterprise Virtualization Guest 6.1, 6.2, 6.3  
Red Hat Enterprise Virtualization Guest 6.4 2.6.32-358  
Red Hat Enterprise Virtualization Guest 6.5 2.6.32-431  
Windows Server 2008 Hyper -V

### Tripwire Enterprise / DB

DB2 9.7, 10.1, 10.5, 11.1  
SQL Server 2008 (SP1 - SP4) , 2008 R2 (SP1 - SP3) , 2012 (SP1 - SP3)  
SQL Server 2014, 2016, 2017, 2019  
Oracle 11g R2 (11.2.0.1 - 11.2.0.3), 12c, 12c R2, 18c, 19c  
Oracle RAC 11g R2  
PostgreSQL 9.2 - 9.6

### Tripwire Enterprise / DS

Windows Active Directory 等  
(サポートされるディレクトリサービス製品については、別途お問い合わせ下さい)

### Tripwire Enterprise / ND

Cisco Catalyst 1900 v9.00.07 , Cisco CatOS v8.6 (2)  
Cisco IOS v12.4 (18) , Cisco PIX v6.3 (5) , Cisco PIX v8.0 (2)  
Cisco VPN Concentrator v4.1.7D  
Extremeware Switches v7.7.2 , F5 BigIP v9.1  
Juniper M&T v8.3 R2.8 , Juniper Netscreen 5.4.0 r6.0  
Nortel Alteon v23.2 , Nortel Passport v4.1.2 , Nortel Web OS v10.0.34

詳細なサポートOSは、トリップワイヤ社HPを御覧ください<http://www.tripwire.co.jp/products/enterprise/platform/>



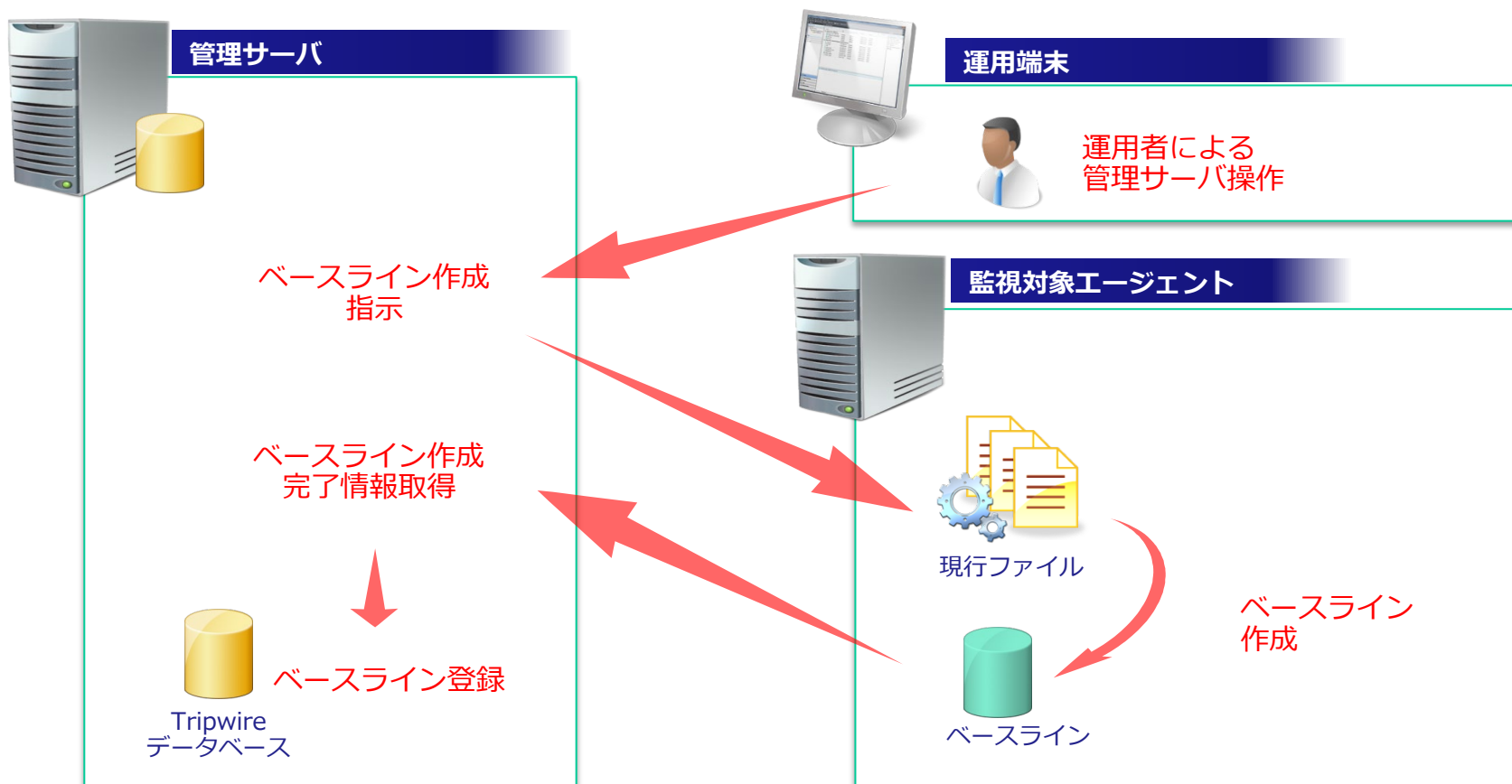
# Contents

---

1. Tripwire Enterpriseのご紹介
2. Tripwire Enterprise活用イメージ
3. Tripwire 製品概要
- 4. Tripwire 製品機能**
5. Tripwire社について
6. 日立ソリューションズ・クリエイトについて

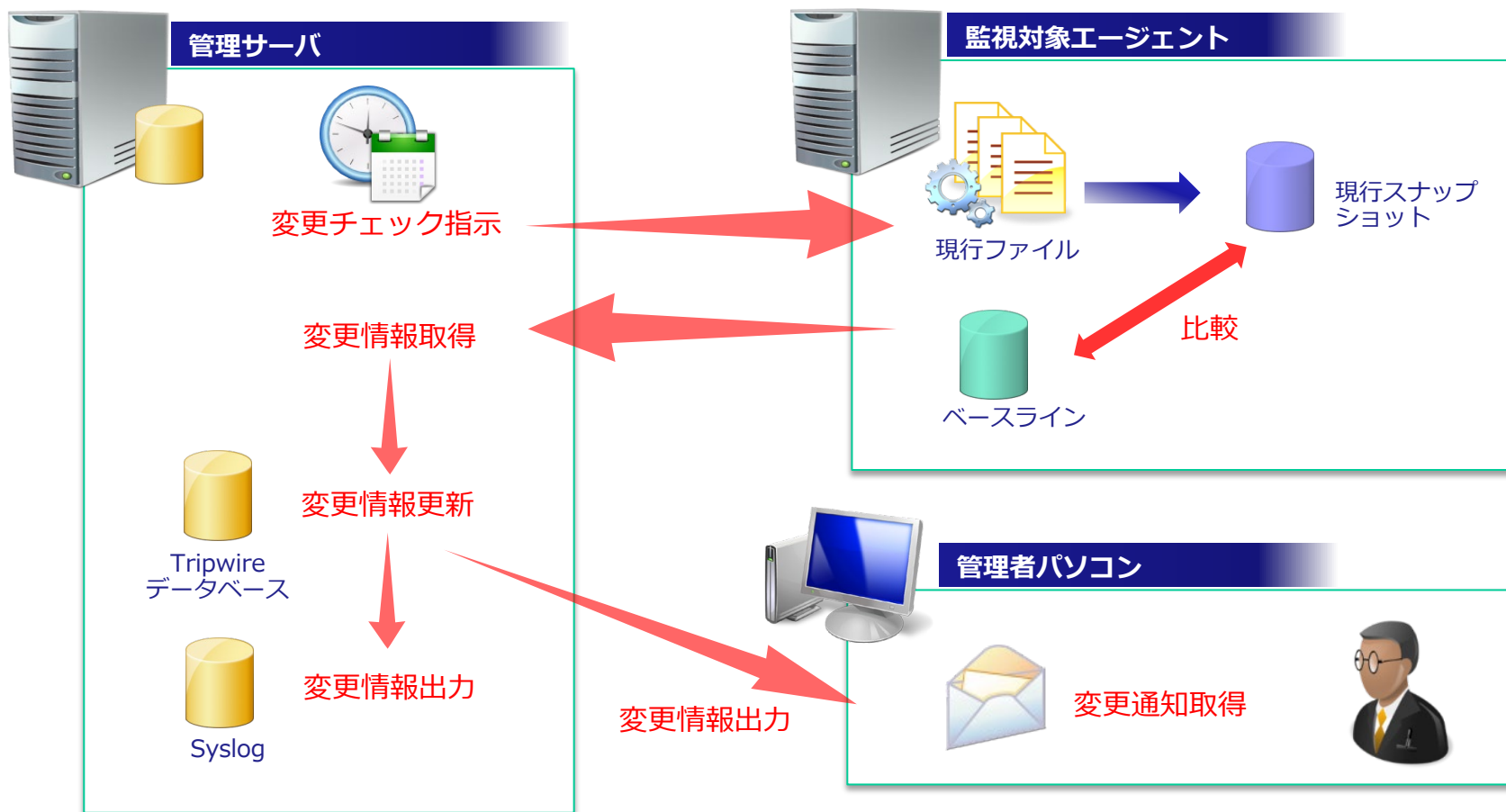
## 製品機能 - ベースライン作成機能

- 管理サーバ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、管理サーバへ結果を返す。
- 管理サーバはベースラインをデータベースに登録する。



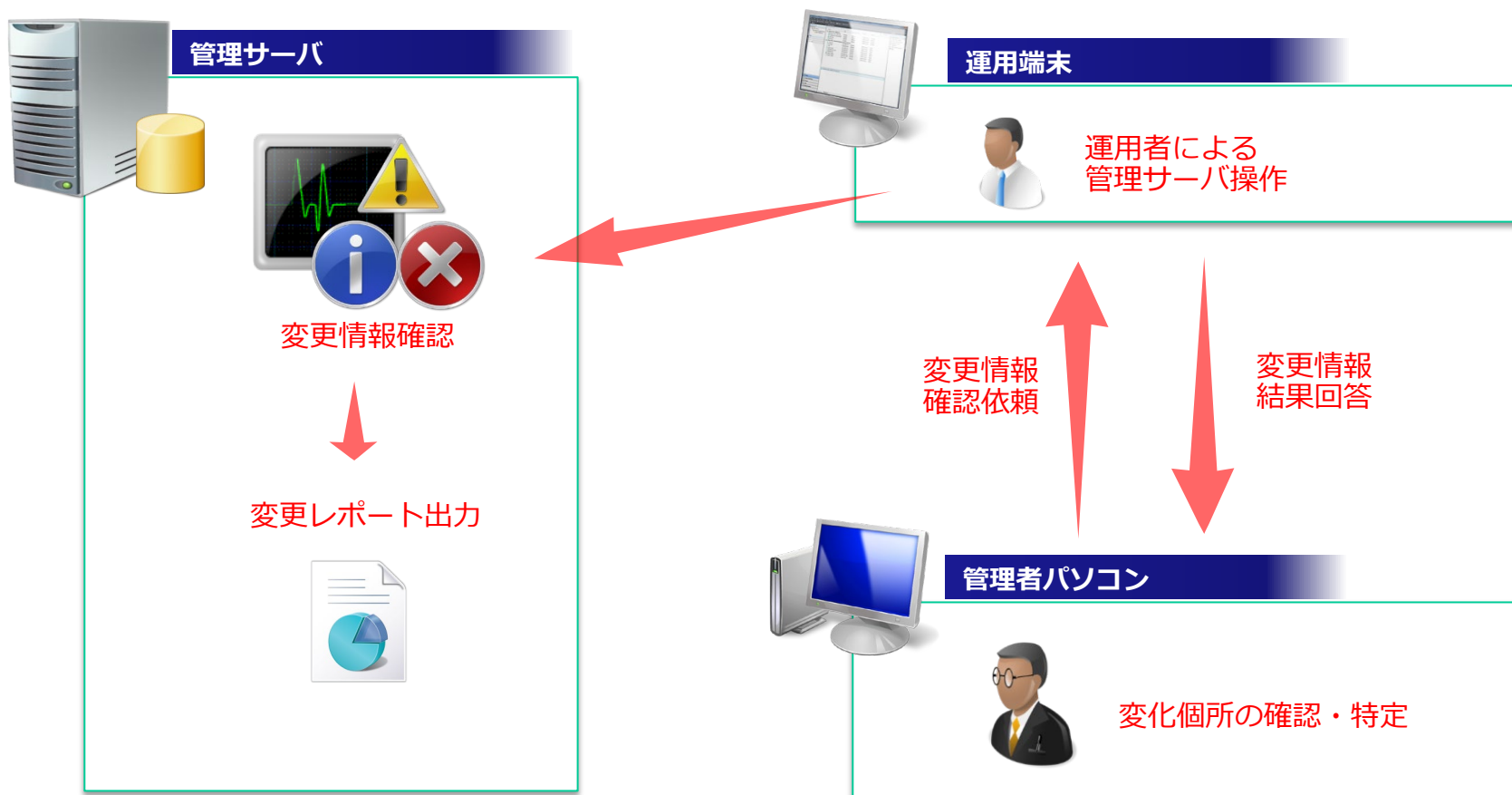
## 製品機能 - 変更チェック機能

- 管理サーバ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へ返す。
- 管理サーバ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する。



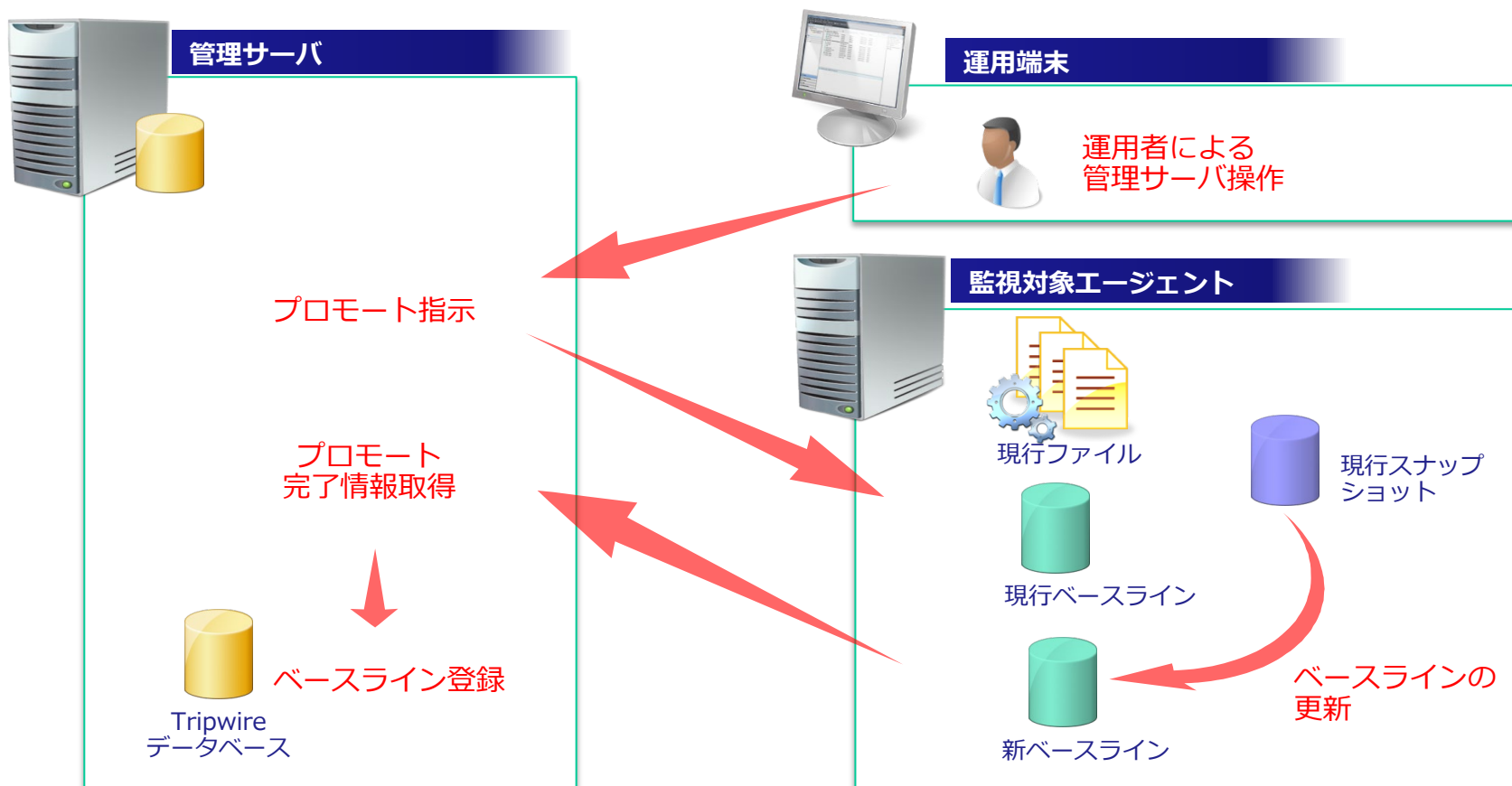
## 製品機能 - 変更情報確認機能

- 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。

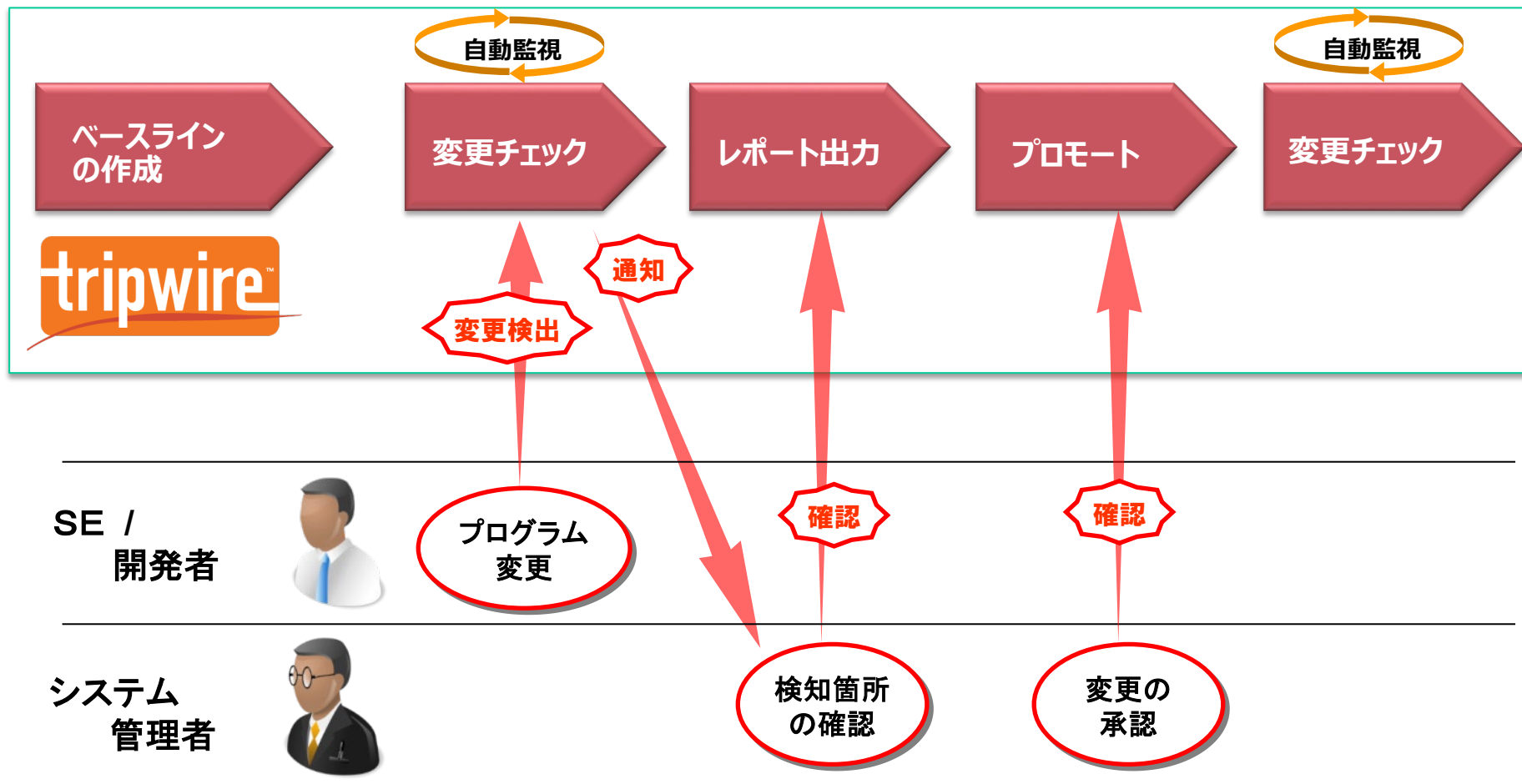


## 製品機能 - プロモート（ベースライン更新）機能

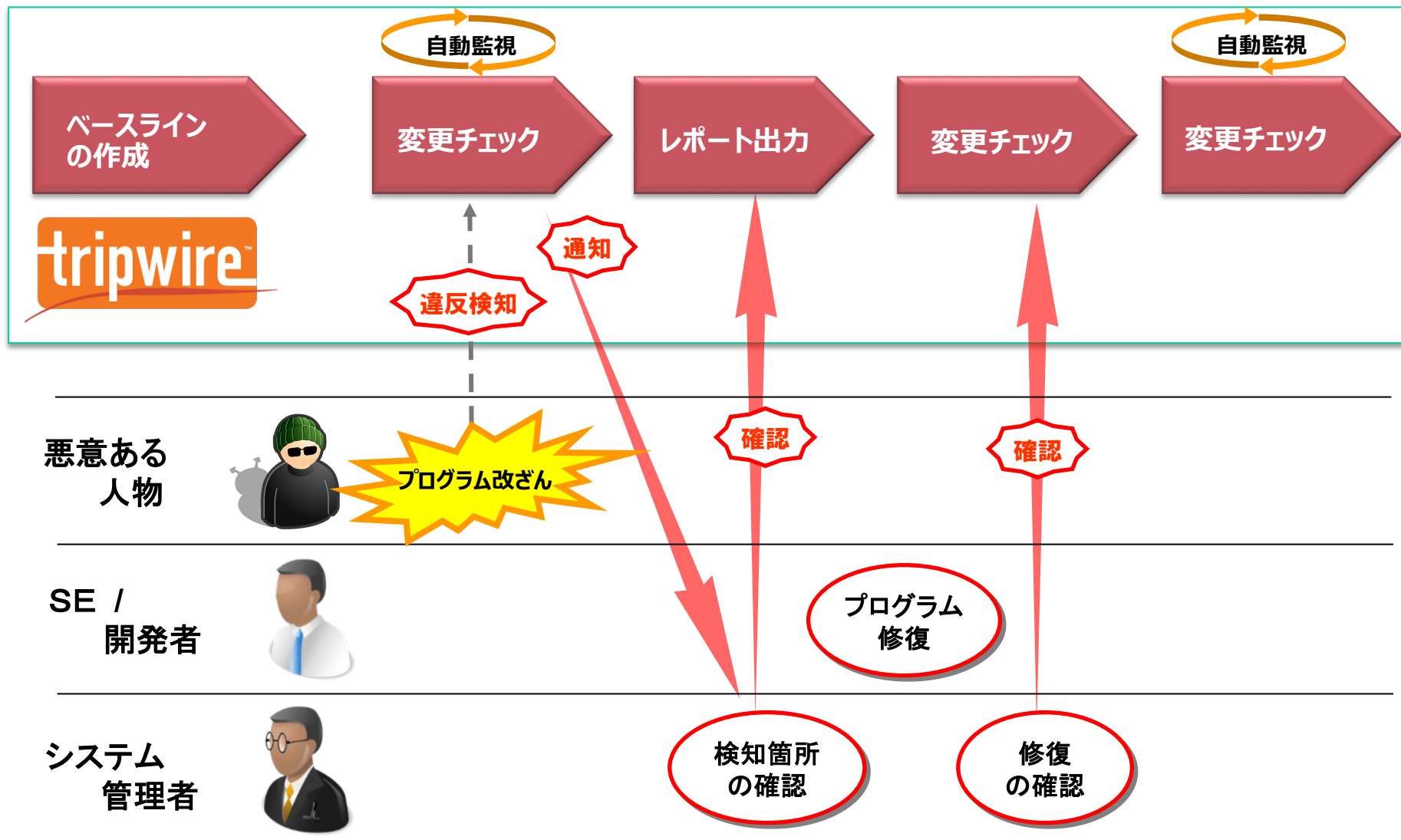
- 管理サーバより監視対象エージェントに対してプロモート指示を行う。
- 監視対象エージェントは新ベースラインを作成し、管理サーバへ結果を返す。
- 管理サーバは新ベースラインをデータベースに登録する。



## ■ プログラム変更時の運用例



## ■ 改ざん時の運用例



# Contents

---

1. Tripwire Enterpriseのご紹介
2. Tripwire Enterprise活用イメージ
3. Tripwire 製品概要
4. Tripwire 製品機能
5. Tripwire社について
6. 日立ソリューションズ・クリエイトについて



### ■ Tripwireの沿革

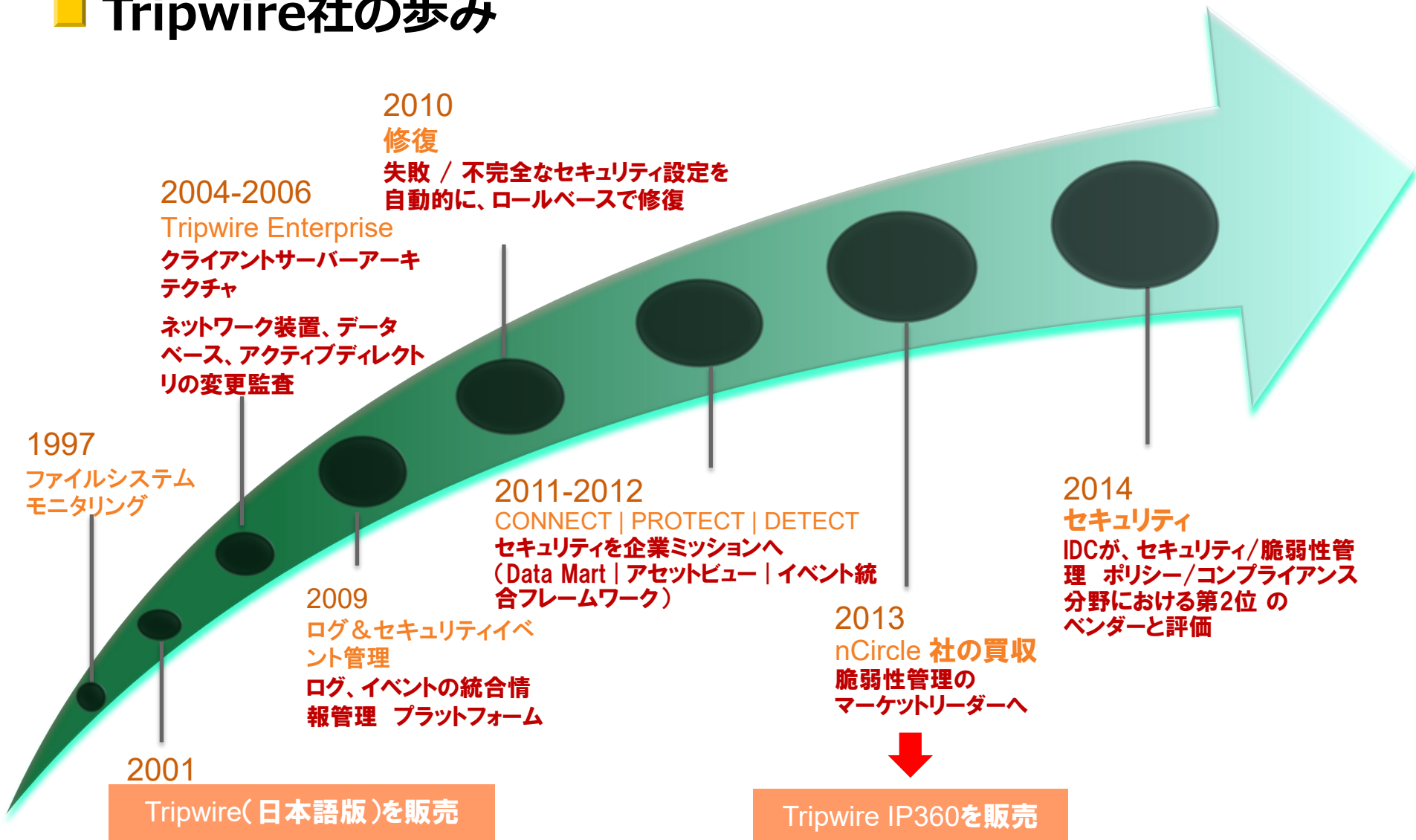
1992年	米国Purdue大学にてTripwire初版開発
1997年	Tripwire, Inc.設立
2000年	トリップワイヤ・ジャパン(株)設立
2001年	Tripwire製品日本語版出荷開始
2006年	Tripwire Enterprise日本語版出荷開始

累計顧客数：約9,000社/団体（世界96カ国）

280,000ライセンスを超えるTripwire製品が現在稼動中



## ■ Tripwire社の歩み



# Contents

---

1. Tripwire Enterpriseのご紹介
2. Tripwire Enterprise活用イメージ
3. Tripwire 製品概要
4. Tripwire 製品機能
5. Tripwire社について
6. 日立ソリューションズ・クリエイトについて

## 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

国内代理店で唯一

(2017年5月時点)

### 豊富な大型案件の導入実績

TRIPWIRE®  
**ENTERPRISE** 導入事例

- ◆ 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

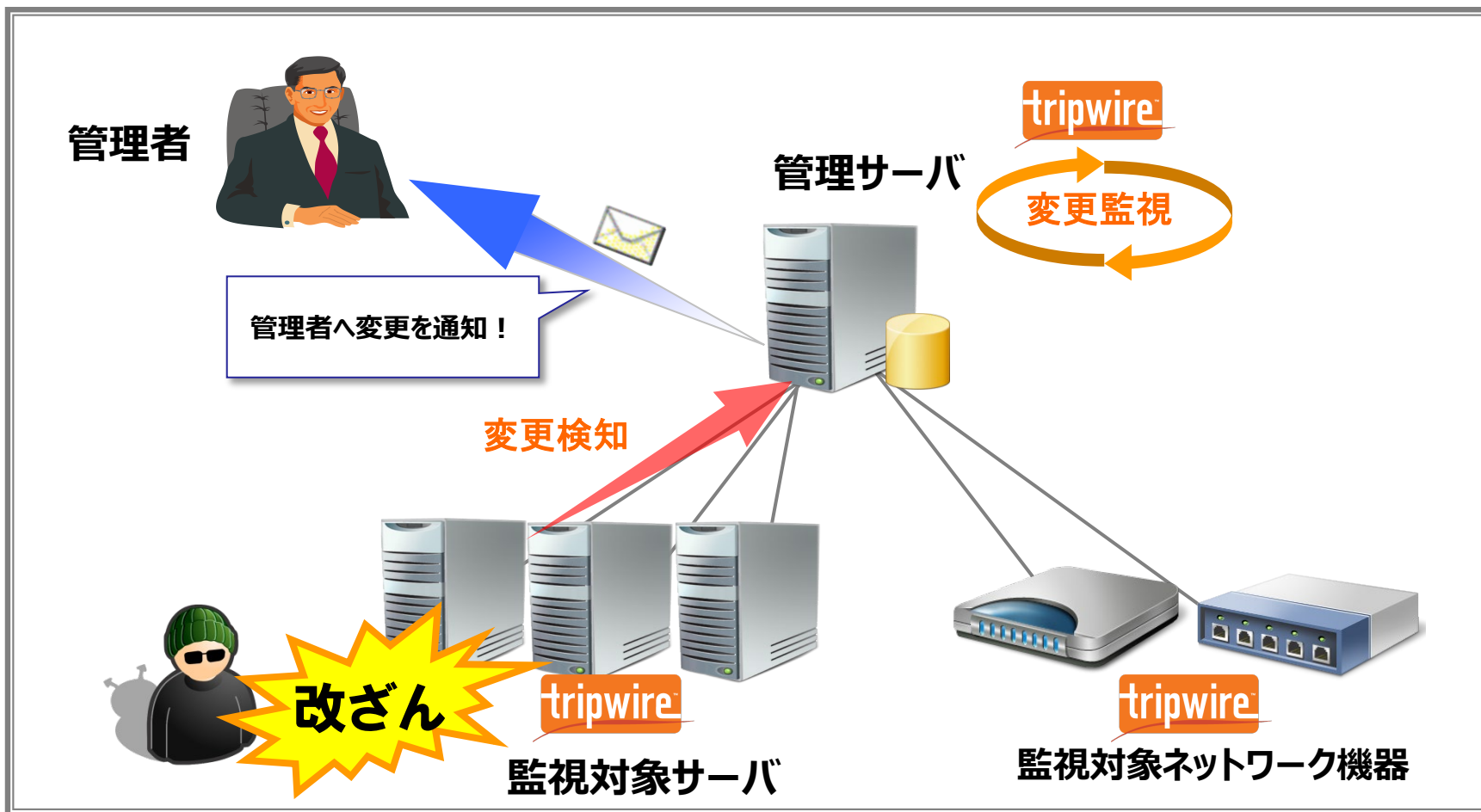
## 導入事例

項	お客様	業種	導入目的	導入規模
1	信販系カード会社 A社様	金融業 (クレジットカード)	PCI DSS (v1.2) 対応 PCI DSS (v3.0) 対応	マネージャ：1台 監視対象：サーバ15台
2	銀行系カード会社 B社様	金融業 (クレジットカード)	PCI DSS (v2.0) 対応 PCI DSS (v3.2) 対応 改竄検知	マネージャ：2台 監視対象：サーバ210台
3	銀行系カード会社 C社様	金融業 (クレジットカード)	PCI DSS (v2.0) 対応 PCI DSS (v3.0) 対応	マネージャ：2台 監視対象：サーバ100台、仮想環境3台 ネットワーク機器35台
4	大手クレジットカード会社 D社様	金融業 (クレジットカード)	PCI DSS (v2.0) 対応	マネージャ：2台 監視対象：サーバ15台
5	鉄道業 E社様	鉄道業	PCI DSS (v3.0) 対応	マネージャ：2台 エージェント：100台
6	メガバンク F社様	金融業 (銀行)	改竄検知 変更管理	マネージャ：3台 監視対象：サーバ100台
7	政府系金融機関 G社様	金融業 (政府系金融機関)	改竄検知	マネージャ：2台 監視対象：サーバ20台
8	郵便業 H社様	郵便業	改竄検知	マネージャ：3台 監視対象：サーバ70台
9	生命保険 I社様	保険業	SOX法対応	マネージャ：2台 監視対象：サーバ200台 ネットワーク機器20台

Security

# Web改ざん検知システム

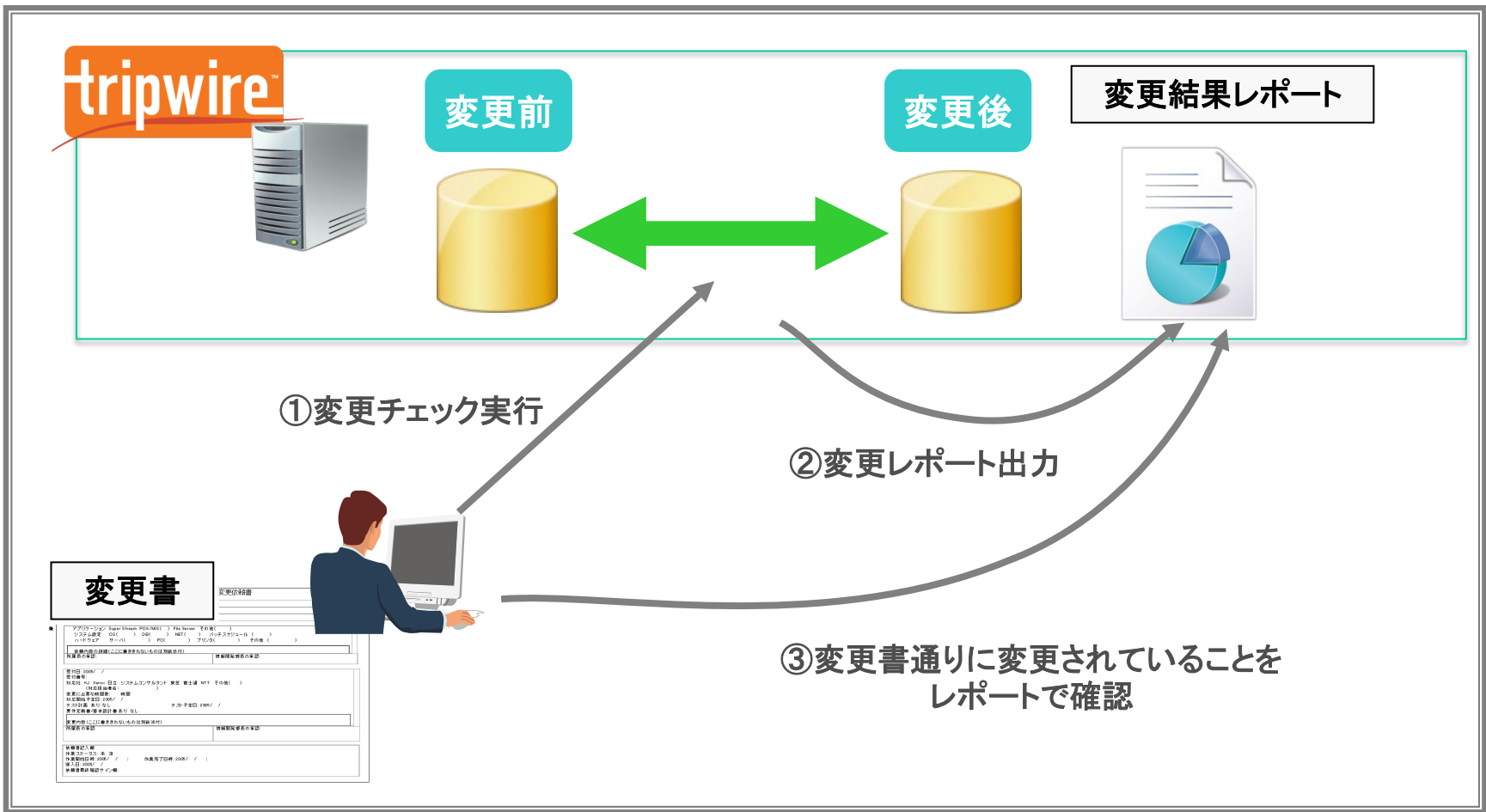
既知の変更，未知の変更（改ざん）されたファイル名を正確に検知・通知します。



Availability

システム変更チェックシステム

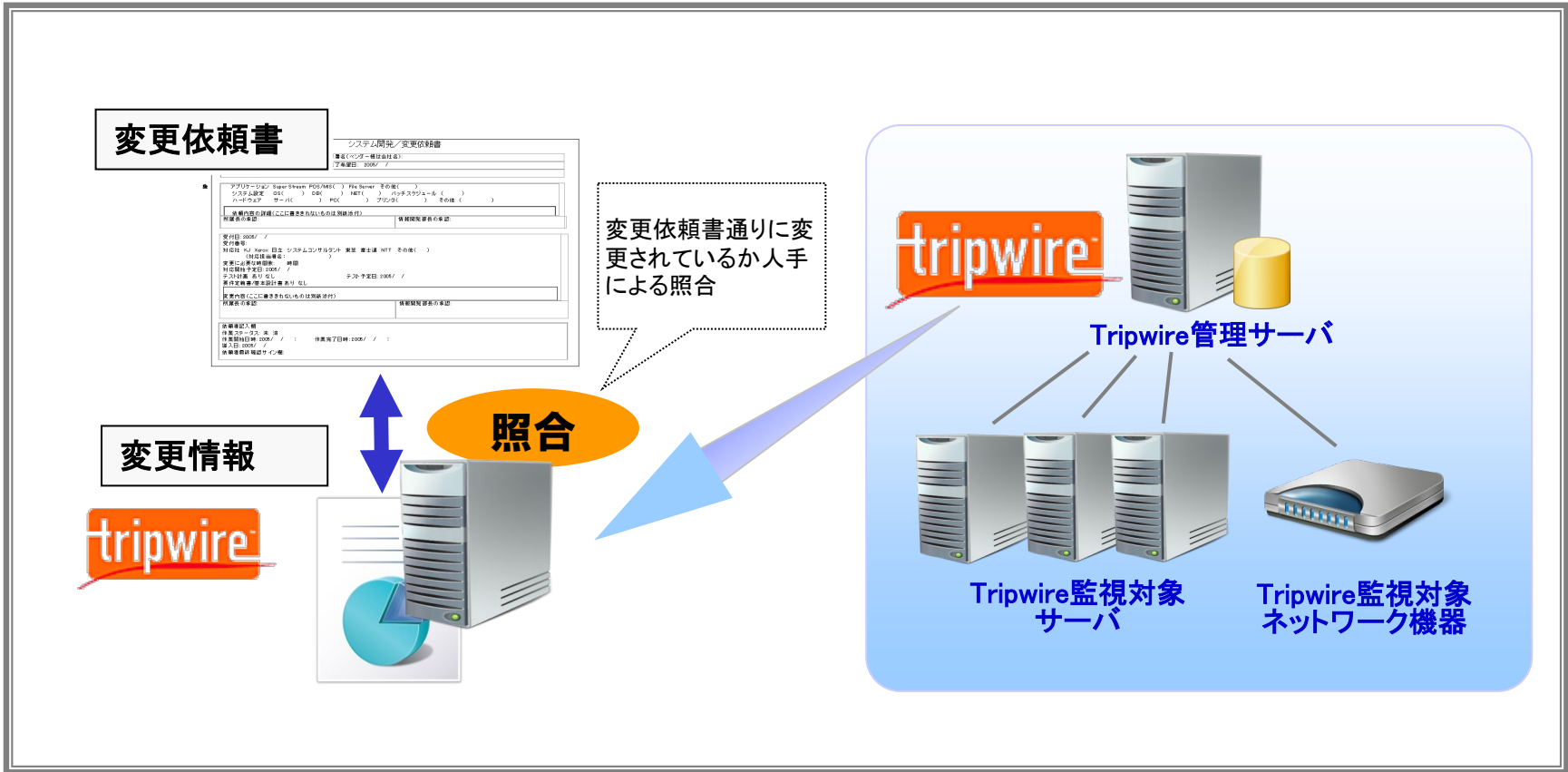
意図した変更が的確に実施されたか、結果レポートで確認します。



## 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。



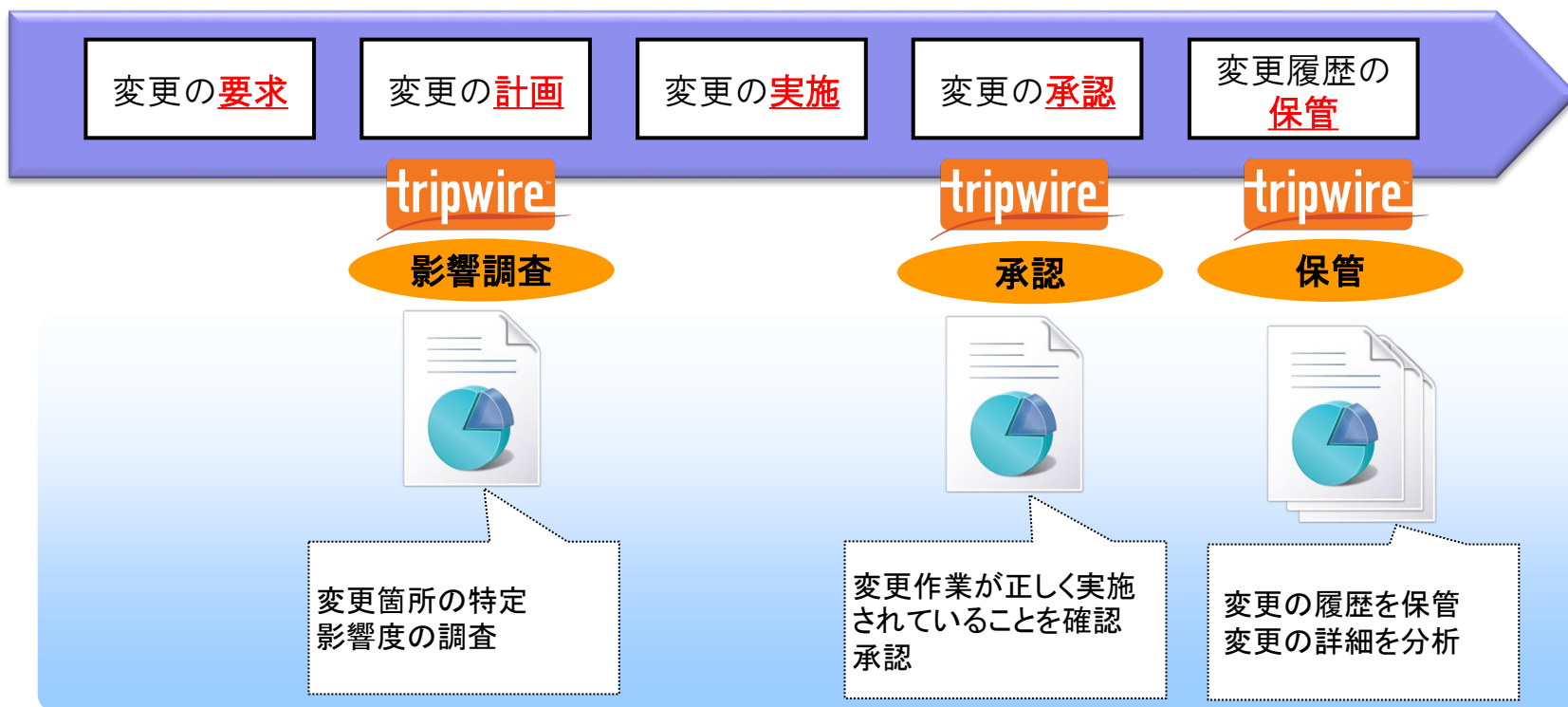


## Compliance

## 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、変更の検知／変更の評価／変更の承認／変更履歴の保管を効率的に支援します。

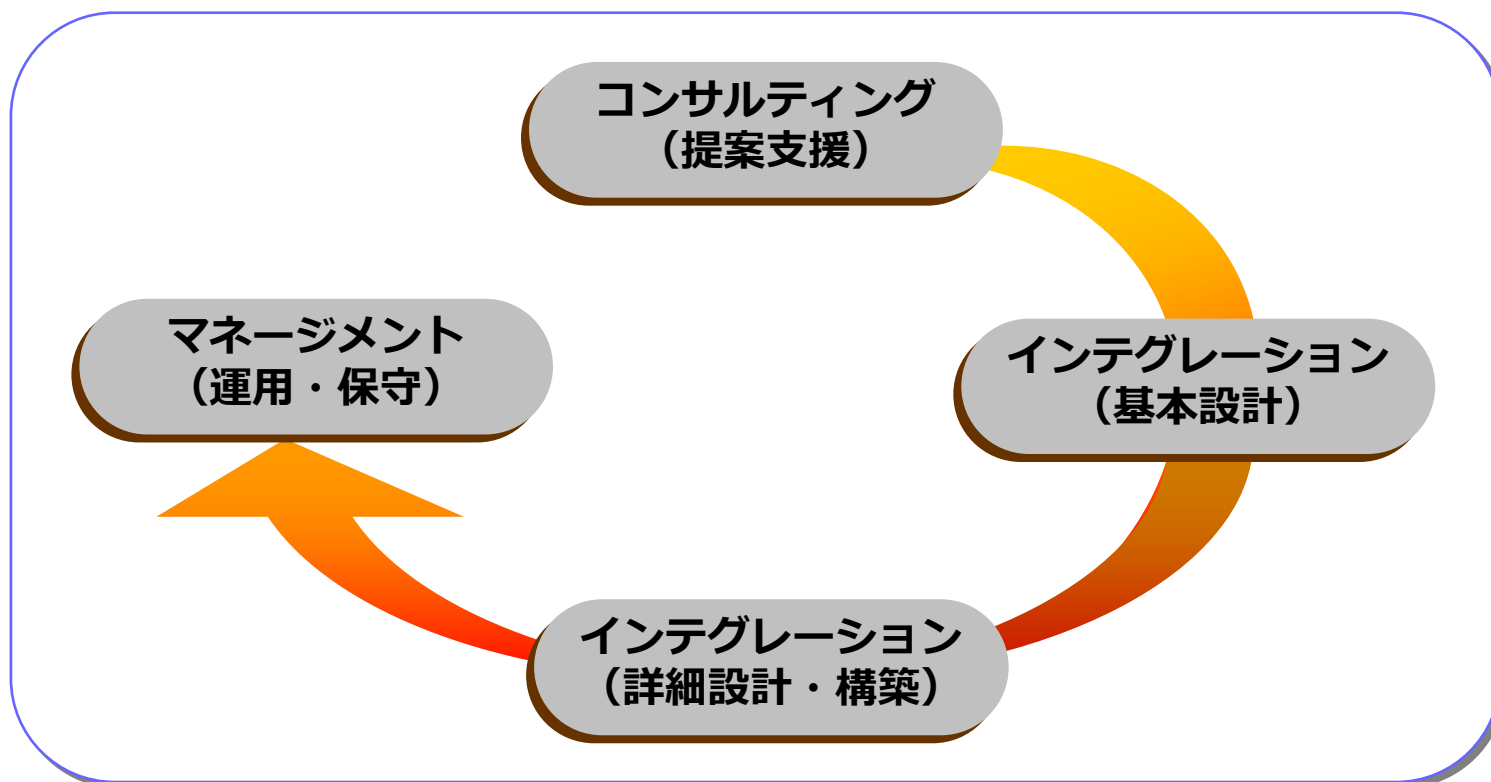
## 変更管理プロセス



### ● 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、提案支援から設計・構築・運用保守に至るまでの各種ソリューションを提供します。

Tripwire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・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, デモ実施を行います。 導入を検討しているお客様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。
マネージメント (保守・運用)	操作教育サービス	Tripwire 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, 削除等の環境再設定の支援を行います。

## 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/inq.html](http://www.hitachi-solutions-create.co.jp/inq.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](mailto:hsc-contact@mlc.hitachi-solutions.com)

- Tripwireは、Tripwire Inc.の登録商標です。
- UNIXは、X/Open Company Limited が独占的にライセンスしている米国ならびに他の国における登録商標です。
- AIXは、米国における米国International Business Machines Corp.の登録商標です。
- HP-UXは、米国Hewlett-Packard Companyのオペレーティングシステムの名称です。
- 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。
- Solarisは、米国Sun Microsystems, Inc. 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。
- Microsoftは、米国およびその他の国における米国Microsoft Corp.の登録商標です。
- Windowsは、米国およびその他の国における米国Microsoft Corp.の登録商標です。
- Windows Serverは、米国およびその他の国における米国Microsoft Corp.の商標です。
  
- その他記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。