tripwire
CONFIDENCE: SECURED

ファイル整合性監視といえばトリップワイヤ でもそれだけではもったいない！　【配布用サマリー版】

トリップワイヤ・ジャパン株式会社
2016年6月22日

本日ご紹介する内容

Item 01　トリップワイヤ　会社紹介

Item 02　PCI DSSの歴史と『改ざん検知』Tripwire

Item 03　『改ざん検知』だけじゃないTripwire Enterprise

Item 04　Tripwire Enterpriseによる監査対応

1. トリップワイヤ　会社紹介

トリップワイヤ　会社概要

本社：米国オレゴン州ポートランド　1997年設立
トリップワイヤ・ジャパン株式会社　2000年設立
（100%出資の子会社）

導入実績：世界96カ国 9,000社
- Fortune 500社の 50%が顧客

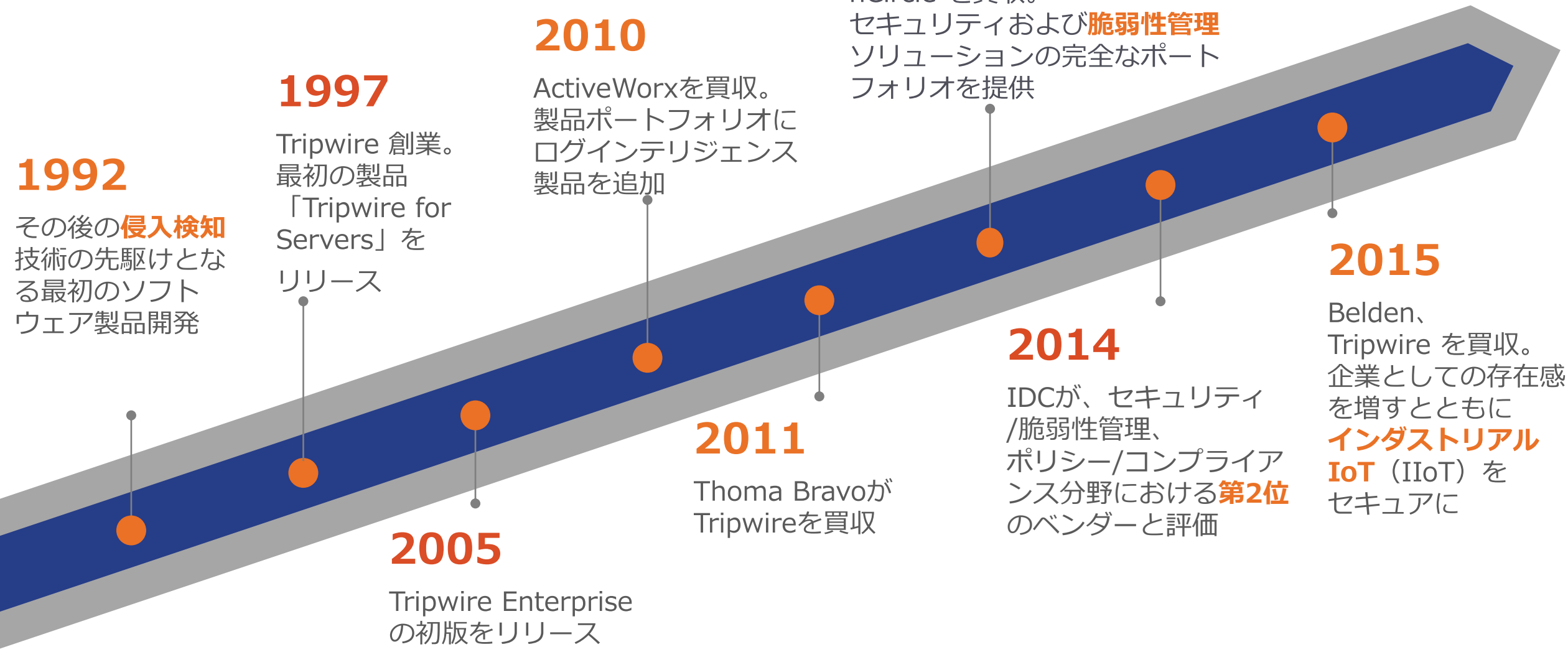
導入実績：日本 1,000社（官公庁・一般企業・etc）
- IPAウェブサイトでWeb改ざん検知製品として紹介
- PCI　認定スキャンベンダーとして
  日本カード情報セキュリティ協議会で紹介

TRIPWIRE® ENTERPRISE

TRIPWIRE® IP360

- **変更検知に特化して15年**
- **変更検知のパイオニアであり、デファクトスタンダード → No.1 のマーケットシェア**

Tripwireの沿革



1992

その後の**侵入検知**技術の先駆けとなる最初のソフトウェア製品開発

1997

Tripwire 創業。最初の製品「Tripwire for Servers」をリリース

2005

Tripwire Enterprise の初版をリリース

2010

ActiveWorxを買収。製品ポートフォリオにログインテリジェンス製品を追加

2011

Thoma BravoがTripwireを買収

2013

nCircle を買収。セキュリティおよび**脆弱性管理**ソリューションの完全なポートフォリオを提供

2014

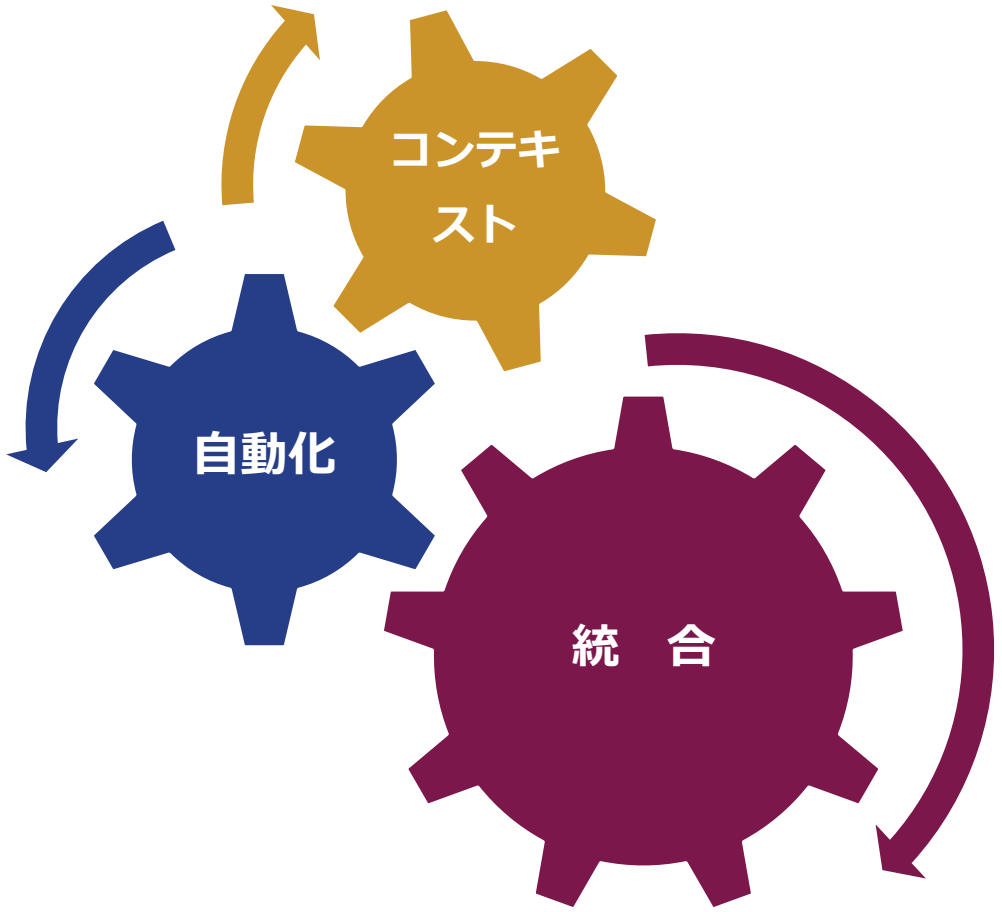
IDCが、セキュリティ/脆弱性管理、ポリシー/コンプライアンス分野における**第2位**のベンダーと評価

2015

Belden、Tripwire を買収。企業としての存在感を増すとともに**インダストリアル IoT**（IIoT）をセキュアに

セキュリティ/コンプライアンス/ITオペレーションをサポート

統合と自動化が、敏捷性と効率性をもたらす



プロアクティブな脅威防御

- 攻撃対象領域の低減
- 新たな脅威の発見

継続したコンプライアンス

- ビジネスの俊敏性
- リソースの最適化

迅速なITオペレーション

- ビジネスリスクの低減

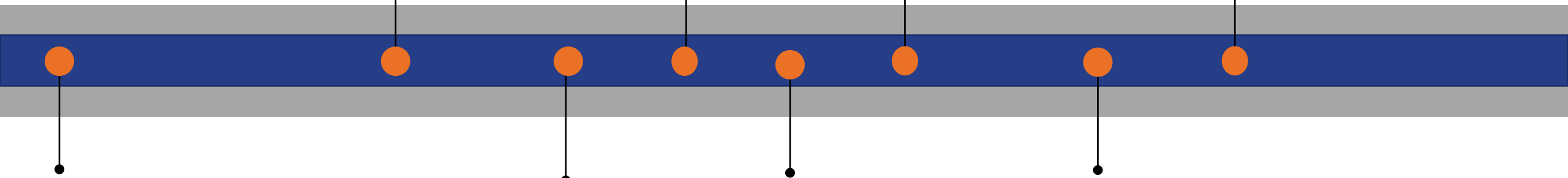
Tripwire Enterprise認定SEの推進

Certified Operator、Certified Professional、Certified Consultantの3種

- **認定SEを活用しての導入を推奨**
- **展開時の迅速性**
- **導入後の安定稼動**
- **高品質なサポート**

2. PCI DSSの歴史と
『改ざん検知』Tripwire

PCI DSS タイムライン



1999

VISA がカード会員情報セキュリティプログラム（CISP）を承認

2004 年 12 月

PCI DSS 1.0 – **Tripwire** が例として記載

2006 年 9 月

PCI DSS v1.1 – PCI カウンシルの設立

2008 年 10 月

PCI DSS v1.2 – WiFi、AV 追加

2009 年 7 月

PCI DSS v1.2.1

2010 年 10 月

PCI DSS v2.0 – 主に明確化

2013 年 11 月

PCI DSS v3.0 – 変更、新たな要件、ロギングの拡張

2015 年 4 月

PCI DSS v3.1 – 暗号化について更新

PCI DSSにおけるファイル整合性監視への要求

PCI DSS 3.1ベース

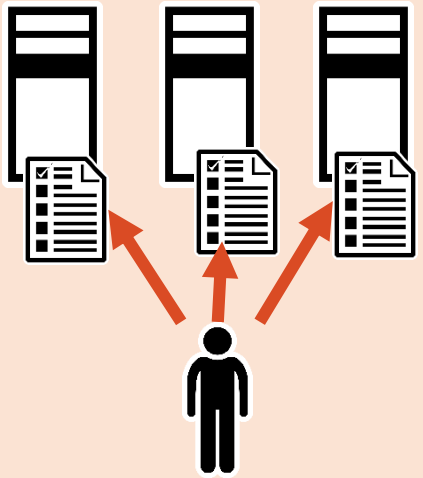
- **通常のプロセスに実装するベストプラクティス**
  セキュリティコントロールの監視 - ファイアウォール、侵入検知/侵入防止システム（IDS/IPS）、**ファイル整合性監視（FIM）**、アンチウイルス、アクセスコントロールなど - 意図されたとおり効果的に動作するようにする。
- **10.5.5** ログに対して**ファイル整合性監視**または**変更検出ソフトウェア**を使用し、既存のログデータを変更すると警告が生成されるようにする（ただし、新しいデータの追加は警告を発生させない）。
- **10.6.1** セキュリティイベントを日々確認する。例：不審または異常なアクティビティを識別する通知または警告。重要なシステムコンポーネントからのログ。ファイアウォール、IDS/IPS、**ファイル整合性監視（FIM）**システムなどのセキュリティ機能を有するシステムからのログ。
- **11.5 変更検出**メカニズム（**ファイル整合性監視ツール**など）を導入して、重要なシステムファイル、構成ファイル、またはコンテンツファイルなどの不正な変更（変更、追加、削除など）を担当者に警告し、重要なファイルの比較を少なくとも週に一度実行するようにソフトウェアを構成する。
- **12.10.5** セキュリティ監視システム、侵入検知、侵入防止、ファイアウォール、**ファイル整合性監視システム**などからの警告を含める。

オープンソースで可能な監視

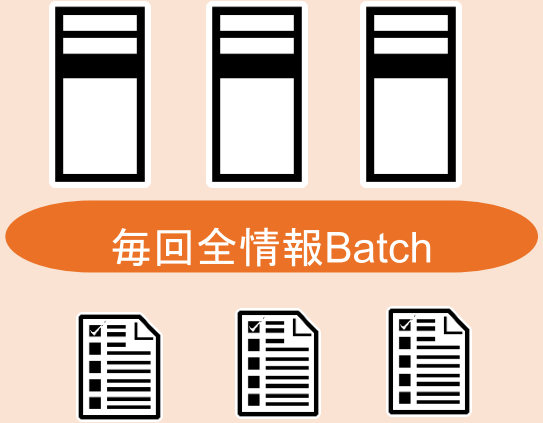
組織にマッチしているか？

Check!
『Tripwire』と見たときには
オープンソースであるかどうかを
確認！

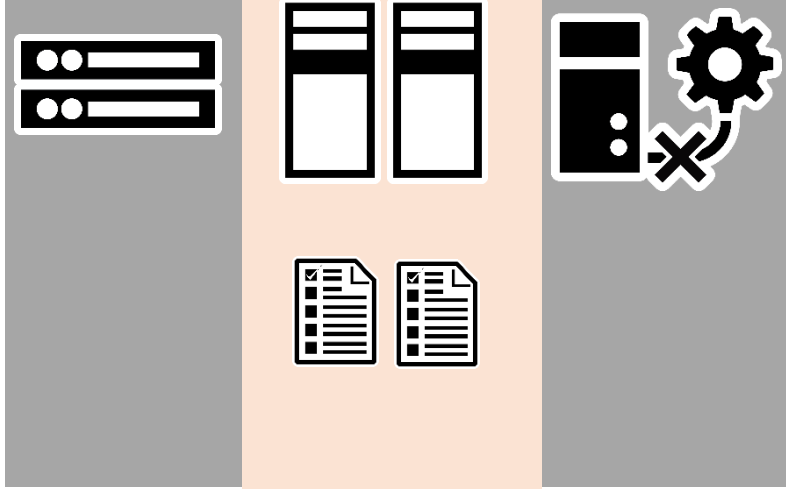
ノードが数台



定期的に監視



プラットフォームの種類が限定



3. 『改ざん検知』だけじゃない
Tripwire Enterprise

企業ニーズを取り込んだ　Tripwire Enterprise

OSS Tripwireをベースに、企業規模や環境にあう運用を可能に

リアル
タイム監視

一元管理

サポート

広範な
管理対象

定期監視

ポリシー
管理

環境に合わせた運用
運用効率化、運用コスト低減、安心/安全稼動
強固なセキュリティを包括的に提供

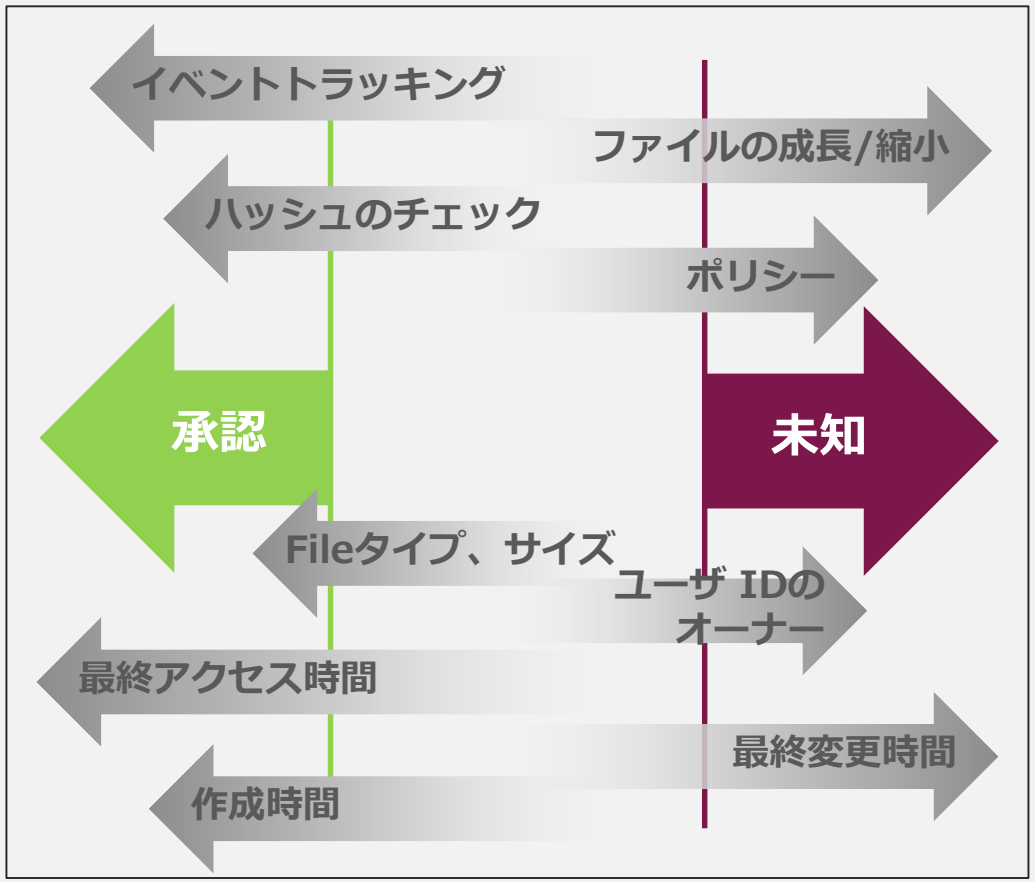
Tripwire Enterprise ～改ざん検知　+α

整合性管理

ポリシー管理

整合性管理

対応管理



TRIPWIRE® ENTERPRISE

- ベースラインを活用した逸脱検知 – 変更を理解
- リアルタイムでの変更検知も実現
- 即対応が必要なものを見分けるため　ChangeIQ機能がノイズを削減
- サイバー犯罪制御 – すぐに使える侵害検知ルールの提供
- 脅威、変則的なものへの指標

Tripwire Enterprise ～改ざん検知　+α

ポリシー管理

整合性管理

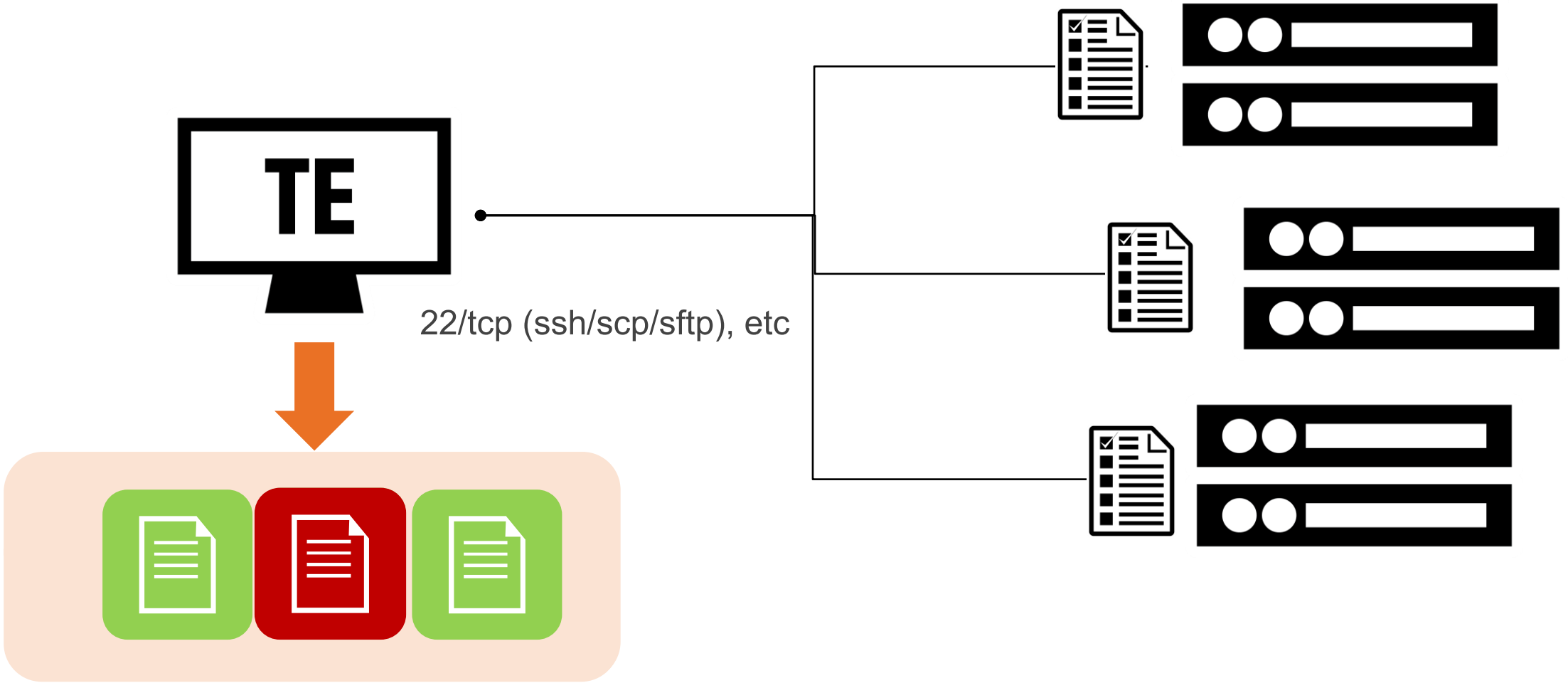
対応管理

TRIPWIRE® ENTERPRISE

- 400以上のセキュリティ/コンプライアンスポリシーを持つライブラリ
- 変更があった際、ポリシーと比較
- 通常とは異なる変更の識別を自動化
- 継続可能
- 迅速で、効果的な監査

改ざん検知はサーバだけのもの？！

たとえばNetwork Deviceも監視対象



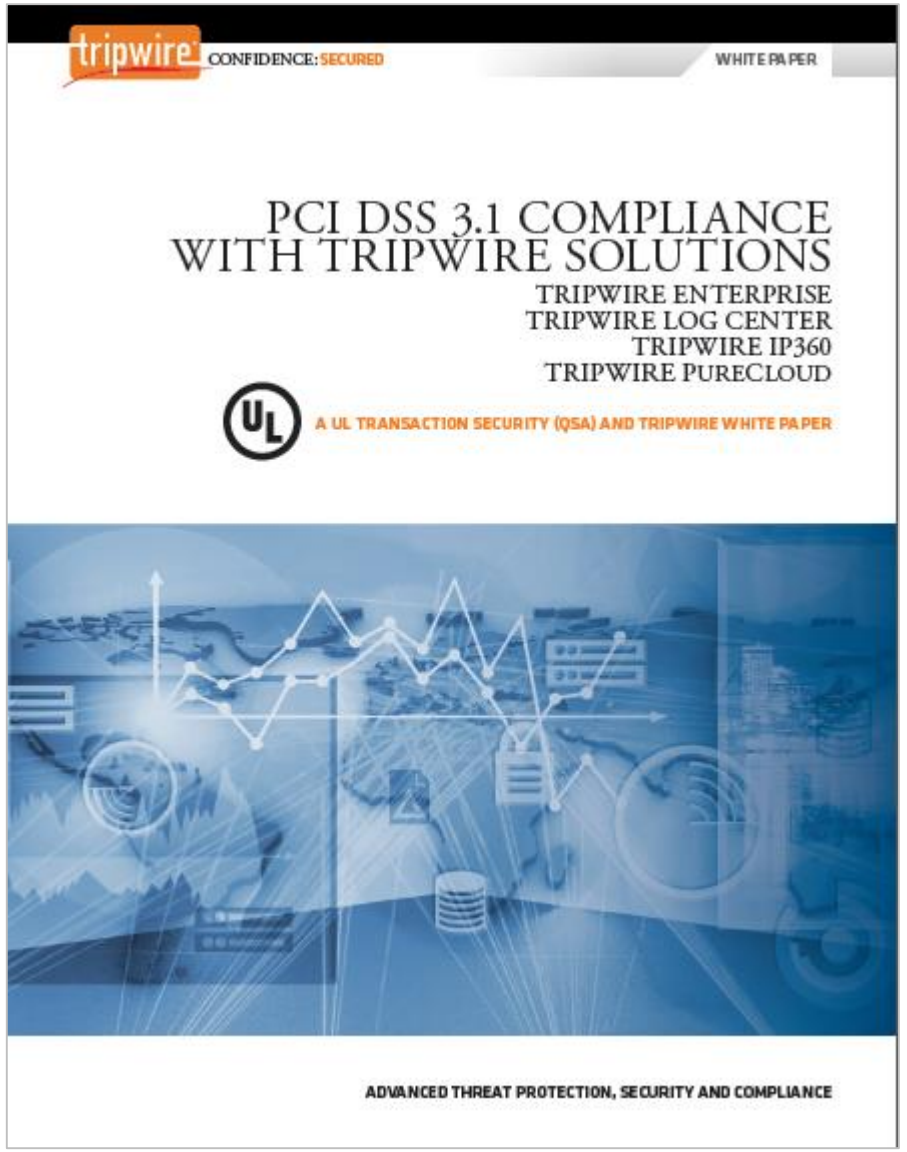
4. Tripwire Enterpriseによる監査対応

トリップワイヤの製品はQSAにより評価

高度なセキュリティを提供しつつ　監査にも強い

- QSA　UL Transaction Security Division
- Tripwire製品機能とPCI DSS要件

TRIPWIRE® ENTERPRISE	TRIPWIRE® IP360	TRIPWIRE® PURECLOUD
33	8	4



Tripwire Enterprise　機能は大きく２つ

- ファイル整合性監視（FIM）
  - File Integrity Monitoring
- コンプライアンス・モニタリング
  - Policy Manager

4

２９

TRIPWIRE® ENTERPRISE	TRIPWIRE® IP360	TRIPWIRE® PURECLOUD
33	8	4

PCI DSSの監査をパスする対策
そしてセキュリティを強化したい！

↓

PCI DSS対策について
ぜひトリップワイヤまで
お問い合わせください

tripwire®

CONFIDENCE: SECURED

THANK YOU

〒112-0014
東京都文京区関口1-24-8 東宝江戸川橋ビル8F
TEL : (03) 5206-8610 FAX: (03) 5206-8613

お問い合わせ先： https://www.tripwire.co.jp/contact