SOLUTION brief

PCI DSS　コンプライアンスの達成と維持

Tripwire® Enterpriseのソリューションを活用したコンプライアンスとリスク削減

SOLUTION brief

はじめに

PCI DSSのコンプライアンス要求が高まっています。なぜでしょうか。
端的に言うと重要データの漏洩事件の増大が原因です。このような情報漏洩事件には外部からの悪意のあるセキュリティ攻撃から人的/処理的ミスまでさまざまな原因があります。Forrester Researchではセキュリティ違反から起因する発見、対応、通知などの作業、生産性の低下、機会の逸失、罰金などによってレコード1件に付き$90から$305の費用がかかると計算しています。例えば、TJXでは2007年11月時点でデータ漏洩の予想コストを8月の1億6800万ドルから2億1,600万ドルに上方修正しました。

経営陣がコストを削減しつつコンプライアンスを達成/維持する方法を模索する現状では、すべてのIT部門においてコンプライアンスの達成は最優先とされるべき課題です。 実際 フォレスター・リサーチ社※ （※ Forrester Research） が2007年10月に発表したレポートでは、「持続可能なITコンプライアンスプログラムの構築はCISOが最優先で取り組むべき5つの課題のうちの1つ」とされています。

PCI DSS基準を遵守することによってシステム、ハードウェア、およびデータをセキュアに保ち、顧客からの信頼および企業としての評価を確保することができます。このためにITシステムを既知の信頼される状態に保つことが非常に重要なのです。どれだけ技術に優れプロセスに注意を払っている企業にとっても、ITシステムを既知の信頼される状態に保つことは非常に困難な課題です。

企業規模の脆弱性に対応しつつ、コストのかからない方法でPCI DSSコンプライアンスを達成するためには何をなすべきでしょうか。

最先端の構成監査/統制ソリューションであるTripwireを導入することによって、企業は重要なITプロセス統制の継続的なテスト/レポーティングの自動化、手動プロセスの削減が可能になり、PCI DSS要件のコンプライアンスを証明する詳細な監査証跡をいつでも提出することができます。

「Tripwire Enterpriseを導入したことにより、PCI DSS 監査要件のコンプライアンスの証明、予定外作業の削減、変更管理プロセスの劇的な向上に成功しました。」
- Ronnell Wegner氏/SVP, Systems, CAPITAL Card Services

Tripwireを活用したPCI DSS コンプライアンスの維持と達成

PCI DSS要件を遵守することによってメンバー、加盟店、およびサービスプロバイダは情報資産を保護し、クレジットカード会社の義務を果たすことができます。このような要件ではファイヤウォール、ルータ、データベースサーバ、POSデバイスが常にPCI DSSを遵守した状態にあることを検証することを要求します。

Tripwire Enterpriseでは面倒な設定の必要なくそのまま使用できるデータセンター向け変更監査/構成分析ソリューションを提供することによって企業によるPCI DSS要件のコンプライアンスを助けます。TripwireではCISのような業界基準やベンチマークを活用して自動的に構成がPCI DSSの要件を満たしているか分析し、リスクのレベルを判断します。その後、継続的かつ微調整可能な変更検知を通じて情報システムを常に既知の信頼できる状態に保ちます。

Tripwireでは既に多くのクレジットカード加盟店、サービスプロバイダのセキュリティ/データ完全性コンプライアンスプログラムに協力しており、このような企業ではPCI DSS監査に何の問題もなく効率的に合格しています。

継続的なコンプライアンスと監査コストの削減

時間と費用の節約

Tripwire Enterpriseでは監査証跡によってコンプライアンスの証明に必要な証拠を簡単に取得できます。洗練されたレポートと自動作成される監査レポートによって監査人は四半期/一年に一回必要とされる検証作業をスムーズに実施できます。これにより罰金による金銭的なインパクトに対する保険がかかり、監査に向けた準備や手動によるテストに必要なリソースを削減できます。

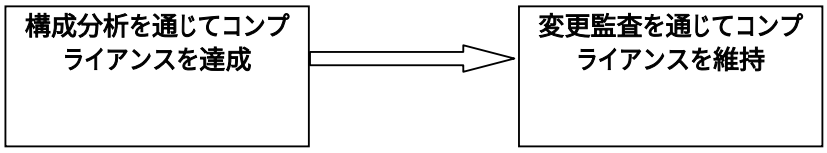
すべての変更を可視化することによってリスクを削減

従来の変更/構成管理ツールでは変更を整然と行うためのプロセスを提供する一方で人的エラーやスタッフや侵入者による未承認の変更に対する防御手段は持ち合わせていません。Tripwire Enterpriseでは変更のソースに関わらずデータセンター内で行われるすべての変更を監視、レポートすることで未承認の変更や基準に違反している構成を検知してセキュリティやコンプライアンス違反の可能性を事前に発見し管理します。

プロセスを常に検証

Tripwire Enterpriseでは変更監査と構成分析の両方の機能を持っており、ポリシーに違反する構成を自動的にレポートすることによって常にコンプライアンスを保ち続けることができます。 TripwireのパワフルなアプローチではCIS (www.cisecurity.org)のベンチマークのような業界基準を活用しています。このベンチマークにはPCI DSSに向けた構成分析も含まれ、自動的にポリシーコンプライアンステストを行うことが可能になります。Tripwireのユニークかつ包括的なアプローチによって情報システムを常に既知の信頼される状態に保つことが可能になります。

Tripwire Enterprise によるPCI DSS コンプライアンスの達成と維持



「監査プロセスを70%近く短縮し、大幅なコスト節約が実現できました。」
- James Summers/Vesta社CISO

「Tripwireを導入したことで、事件が起こってから数分で分析し復旧することが可能になりました。緊急の事態では一分一秒が顧客および我々のビジネスにとって重要な意味を持ちます。」
- Jeremy Dykman/Wesco社のネットワーク/セキュリティマネージャ

PCI DSS要件とTripwire構成監査と統制ソリューション

Tripwireを活用することでPCI DSS要件のうち11要件において様々な条項とのコンプライアンスを達成できます。

PCI 要件	Tripwire の対応
1. ファイヤウォールをインストール/保持してカード保持者のデータを保護する。	Tripwire Enterprise ではファイヤウォールおよびルータの状態を監視し、設定ファイル、ルールセット、必要であればファイヤウォールの基礎をなす OS に対してなされる未承認の変更を検知、対応、報告します。また、Tripwire では期待されるファイヤウォール/ルータ設定基準からの逸脱などの内容を含むレポートを四半期に一回生成し配布することによって、このようなシステムを既知の信頼される状態に保ちます。Tripwire の構成分析テストによって、各デバイスのポリシーへの適合状態をチェックすることができます。
2. システムパスワードやその他のセキュリティパラメータでベンダーが提供するデフォルト値を使用しない。	Tripwire では設定した基準に違反しているすべてのシステム/ネットワークデバイスを検知します。Tripwire Enterprise では構成分析によってサーバ、データベース、ネットワークデバイス、アプリケーションが CIS や PCI DSS のような団体が定める基準や監査ガイドラインを遵守しているかどうかテストできます。
3.保存されるデータを保護する。	Tripwire ではファイルやデータベーステーブルのような特定のタイプのデータの削除を検証、報告することでプロセスを自動化します。
4. 公開されたネットワーク上でカード保持者データを送信する場合は暗号化する。	Tripwire ではセキュリティ設定で必要な構成ファイルを検索して、定義したポリシーから逸脱があった場合はアラートを発します。構成ファイルがコンプライアンスに違反している場合、Tripwire は変更を監視してアラートを発し、変更の検証を行うことができます。すべてのチェックは記録され、継続して行われる監視とレビューの証拠となるレポートを作成することによって監査の手間を省きます。
5. アンチウィルスソフトウェア/プログラムを使用し、定期的にアップデートする。	Tripwire Enterpriseではコンプライアンスに違反したシステムを検知し、アップデートが行われない場合はレポートを出します。 Tripwireのアプローチはコンプライアンスが保たれた状態からの逸脱の検知に依存します。 Tripwire ではシステム変更を追跡、報告し、ゼロデイ攻撃が発生した場合 Tripwire は被害を受けたシステムを検知して、ウィルス定義を利用可能な状態にします。被害を受けたシステムだけを修復することによって、Tripwire では検疫/修復プロセスを短縮/単純化します。
6. セキュアなシステムとアプリケーションの開発と維持	Tripwire Enterprise では実際にインストールされたパッチがインストールを予定されていたパッチと一致するかどうか検証します。パッチ導入プロセスの一部として Tripwire を使用することによって、パッチ適用に失敗した場合のリスクと影響を軽減し、適切なパッチ導入が行われていることを証明する独立した監査証跡を生成します。また、Tripwire では独立した監査メカニズムによって、セキュリティ基準の遵守も保証します。

7. カード保持者のデータへのアクセスを業務上知る必要のある社員だけに制限する。	Tripwire Enterprise では重要なデータへのアクセス権限に変更があった場合はアラートを発し、アクセス権限をアサインされた社員がまだアクセス権限を持っていること、および特定の期間統制がなされていたことを証明できます。
8. コンピュータにアクセスできる各ユーザにユニークな ID をアサインする。	Tripwire Enterprise では新規ユーザ ID や既存のユーザ ID の修正や削除を検知します。
9. カード保持者データへの物理アクセスを制限する。	N/A
10. ネットワークリソースおよびカード保持者データへのすべてのアクセスを追跡および監視する。	Tripwire ソリューションでは企業全体におけるファイル完全性を希望の頻度で監視し、強固かつフレキシブルなレポートを提供します。
11. セキュリティシステムとプロセスを定期的にテストする。	Tripwire Enterprise では構成分析機能を活用して IT システムが設定したベースラインと基準に合致するかどうかテストし、統制が不適切、もしくは存在しない領域を明らかにします。
12. 従業員および請負業者の情報セキュリティ対策を講じるためのポリシーを維持する。	Tripwire Enterpriseではガバナンス文書は作成しませんが、設定した手順を遵守しているかどうか検証することによって、ポリシー違反が発生した場合この違反の証拠を提出します。 Tripwire Enterprise は内部ユーザが未承認の変更を行う場合のようなポリシー違反となる変更を監視し、検知します。

【トリップワイヤ・ジャパン株式会社について】
システムの変更コントロールソフトウェアの製造・販売およびサポートを行う米国トリップワイヤ社 (Tripwire, Inc. 本社 ： オレゴン州ポートランド) 初の現地法人として 2000 年4月、日本に設立されました。トリップワイヤ・ジャパンは変更管理によりセキュリティ強化、可用性向上、コンプライアンスの証明を実現する『Tripwire Enterprise』、改ざん検知のパイオニア製品となった『Tripwire for Servers / Tripwire Manager』の販売・開発・サポートサービスを行っています。累計顧客数はワールドワイドで2008年7月現在、約6,000社/団体以上、ライセンス数では280,000を超えるTripwire製品が稼動中です。

※本ソリューション概要は米国Tripwire, Inc.による PCI DSS ソリューション概要を翻訳したものです。
※本資料についてのお問い合わせは mktg@tripwire.co.jp 電話 03-5306-8610 までお願い致します。