FORTRA™

ソリューション・ブリーフ (TRIPWIRE)

Tripwireによる自動化された継続的なPCI 4.0準拠

顧客カードデータの包括的な保護

PCI データセキュリティスタンダード(PCI DSS)は、クレジットカードデータ決済を処理する組織がカード会員の環境を安全に保ち、クレジッセキュリティ、サイバー脅威、その他のセキュリティの脆弱性を防止するために策定されました。最新バージョンである4.0は、個人情報および金融情報の盗難、暴露、および漏洩を最小限に抑えるため、クレジットカードデータの取り扱い、処理、送信、および保存に関する具体的なセキュリティガイダンスを提供しています。クレジットカード取引を処理する企業は、2024年3月までにPCI 4.0の新しい要件に準拠する必要があります。

攻撃のターゲット:
カード保有者のデータ

2019年の中間検証でPCI DSSへの完全準拠を達成した組織はわずか27.9%にとどまりました。予想通り、小売業界では、インシデントの99パーセントが金銭的な動機によるものであり、決済データは依然として脅威行為者が最も求め、利益を得る商品となっています。このレポートによると、現在ではPOS(販売時点情報管理)デバイスではなく、ウェブアプリケーションが小売業における侵害の主な原因となっています。

—Verizon *2019 Payment Security Report*

挑戦

クレジットカードデータと処理するシステムは、依然として攻撃者には価値のある標的です。調査や多くの科学調査によると、攻撃者が組織の防御を突破するのにかかる時間はわずか数秒から数分ですが、侵入を発見するのに平均して約8カ月かかり、その間に数百万件の記録が流出している可能性があります。ランサムウェアの脅威が増加し続ける中、セキュリティ基準の最低基準を提供する必要性はさらに高まっています。

目標:継続的なPCIコンプライアンスとセキュリティ

残念ながら、多くの組織は、PCIコンプライアンス監査に合格するための「チェックボックス」的な考え方に注力しており、慌ただしい事務手続きの後、通常どおりの業務に戻ってしまいます。これは、ある時点ではサードパーティの侵入テストや脆弱性評価を受けて監査に合格していたとしても、構成がコンプライアンスから「逸脱」してしまう可能性があることを意味します。ITセキュリティーの専門家であれば理解している通り、最低限のコンプライアンス基準に準拠するだけでは、セキュリティーの保証にはなりません。一方、PCI v4.0基準は、継続的なコンプライアンスとセキュリティー監視の実施を求めています。PCI DSSは、企業の全体的なセキュリティー戦略の一環としてBAU(通常業務)活動に導入する必要があります。このようにコンプライアンスとセキュリティに継続的に焦点を当てた運用を行うことで、システムインテグレティーが向上し、リスクが低減します。

PCI DSS 4.0準拠のハイライト

すでに PCI 3.2.1に準拠している場合でも、v4.0への移行にはさらなる労力が必要です。Fortra's Tripwire には、PCI 3.2.1 準拠を合理化し、4.0への準備を判断するツールがあります。4.0の変更対象範囲が広いため、組織の運用プロセスの変更に時間がかかる可能性があります。Tripwireでは、2024年3月に発効される新基準に対応するための計画期間を最大限に確保するため、更新された基準を早期に確認することを推奨しています。

Tripwire's PCIコンプライアンス・ソリューション

Tripwireは、業界をリードする継続的なPCIコンプライアンスと自動化を提供するドメインエキスパートであり、加盟店、銀行、決済処理機関が包括的なPCIセキュリティーポリシーを作成、実施するための製品やサービスを提供しています。Tripwireのソリューションは、クレジットカードのデータを保存しているすべてのシステムをプロアクティブに検出、強化、保護します。

Tripwireは監査への準備と効果的な対応を支援します

Tripwire®Enterpriseは、受賞歴のあるポリシー管理と緊密に統合されたファイル整合性監視を提供します。

- 変更監査、脅威インジケーター、異常検出に対するリアルタイムアラート
- セキュリティポリシーのための既知の信頼できる構成ベースラインの確立、構成の強化、ドリフトを防止
- 修復ガイダンスの組み込み、ITセキュリティとSOCチームの問題解決を促進
- エージェントレスオプション

Tripwire IP360™による脆弱性アセスメントの提供

- 環境の自動検出によるハードウェアとソフトウェア（スコープ内外を問わない）可視化
- 脆弱性インテリジェンスを利用した環境スキャンで対策が必要なリスクを検出

PCI DSS 4.0 - 6つの目的と12の要件

TripwireのPCIソリューションは、単独で使用することも、組み合わせて使用することも可能で、ファイル整合性監視、セキュリティ設定管理、インテリジェントイベントログ、脆弱性管理を提供します。Tripwire を併用することで、優れたセキュリティ対策を検証・実施する「すぐに使える」という価値の提供、監査にも対応するコンプライアンス・レポートも提供します。

PCI DSS v4.0は2022年3月にリリースされましたが、義務化されるの2024年3月であることにご注意ください。Tripwireは、義務化に先駆けてPCI 4.0の全12要件を完全にカバーできるようにソリューションを準備しています。以下の表は、現在開発中の機能を表しています

		Tripwire Enterprise	Tripwire IP360
目的1：	**安全なネットワークとシステムの構築と維持**		
要件1： ネットワークセキュリティ・コントロールのインストールと維持	不正な変更だけでなく基準に適合した設定変更を継続的に検出し、ファイアウォールのログを収集、ネットワークトラフィックが承認されたプロトコルとルートのみを使用していることを証明します。アクセス可能なサービス、不適切なネットワークトラフィック、監視対象のすべてのネットワークデバイス（ファイアウォール、ルータ、スイッチ）の現在のステータスをスキャンおよびテストし、変更承認システム、ワークフロー、およびプロセスをサポートします 。	✔	✔
要件2： すべてのシステムコンポーネントに安全な設定を適用	アクセス制御、プロトコル設定、監査/ログ設定、特権などの領域に対するセキュリティ構成を自動化して検証し、基準へのコンプライアンスを維持します。トリップワイヤのソリューションは,Peripheral Component Interconnect (PCI)、米国国立標準技術研究所 (NIST)、Center for Internet Security Control (CIS Control) 、国際標準化機構 (ISO) など、業界で認知されたシステム強化基準セキュリティフレームワークに対応しています。	✔	✔
目的2：	**カード会員データの保護**		
要件3： 保存されたアカウントデータの保護	暗号化、キー、データファイル、データベーステーブルの削除や変更をチェックし、レポートします。機密データへの不審なアクセスに対してアラートを生成します。ロギングにより、誰がいつ何を変更したか、アクティビティ履歴、フォレンジック・バリューのための自動記録を提供します。	✔	
要件4： オープンな公共ネットワーク経由でカード会員データを伝送する場合、強力な暗号化で保護	データ暗号化をチェックし、脆弱な暗号化方式が使用されている、暗号化を使用せずにサービスが実行されている、暗号化アルゴリズムが変更されたなどの場合に警告し、その詳細を表示します。設定をコンプライアンスが保たれた状態に戻し、修復するためのアドバイスを提示します。さまざまなアプリケーションおよび OS 内での暗号化の使用に関する証明書、レコード、レポートをチェックします。また、自動化機能とコンプライアンスの証拠となる監査対応レポートを提供し、継続的なモニタリングを実施します。	✔	✔
目的3：	**脆弱性管理プログラムの整備**		
要件5： すべてのシステムとネットワークを悪意のあるソフトウェアから保護	ウイルス対策ソフトウェアがインストールされ実行されていることを検証できます。またコンプライアンスに逸脱した状態で実行されているシステムを検出します。システム変更の追跡、アラート、ロギングおよびレポート生成機能を使用して、影響を受けたシステムを検出することで、ゼロデイ攻撃にも効果的に対応します。	✔	✔
要件6： 安全性の高いシステムとアプリケーションの開発と保守	セキュリティ要件や監査要件に合わせてカスタマイズされたルールとテストにより、開発環境と本番環境の変更管理手順を実施します。システムログを取得し、適切にエラー処理を検証し、安全な暗号化ストレージと通信をチェックします。リリース前の開発・テスト環境において、ロールベースのアクセス制御、PAN（ プライマリアカウント番号）およびその他のカード会員データの保護を目的とした要求に強力に対応します。常に最新の脆弱性情報を提供し、企業がリスクのランクを割り当てる脆弱性管理を提供します。オンプレミス、クラウドでの導入が可能です。	✔	✔

		Tripwire Enterprise	Tripwire IP360
目的4：	**強力なアクセス制御手法の導入**		
要件7： カード会員データへのアクセスを、業務上必要な範囲内に制限	認証、権限の設定を含むアクセス制御の使用および変更の監視に関する補足的な監査証拠の維持を支援します。サードパーティ製品の共通設定およびカスタム設定を検知できます。PCI データを格納するマシンへのローカルログインを監視し、ログイン試行に関するログ情報を収集して不審なログインを検知すると警告します。	✔	
要件8： システムコンポーネントへのアクセスを確認・許可	この要件に対するサブコントロールの多くは、手続的で文書的です。ただ、Tripwire製品 を使用することで、多くの要件を実施、記録、警告することができます。マルチファクター認証およびパスワードポリシーの検証などはコンプライアンス監査機能の一部として提供され、さらに暗号化の強度、認証情報の有効性をチェックし、あらゆる種類のアクセス再試行、解雇された従業員によるアクセス、各従業員の固有IDの検証などに対し警告します。	✔	
要件9： カード会員データへの物理的アクセスの制限	T物理的な監視やアラームソフトウェアに使用されるカスタムアプリケーションの監視機能で、物理的なアクセス制御などのセキュリティ手順をサポートします。典型的な動作以外の検知を自動化できます。アクセス制御メカニズムのログを取得し、他のデータと関連付けることで、不適切な物理アクセスを検出します。		
目的5：	**ネットワークの定期的な監視およびテスト**		
要件10： システムコンポーネントおよびカード会員データへのすべてのアクセスを追跡および監	ログ収集、レポートの生成および保持の要件を満たし、それらを暗号化して安全に保存します。これにより、ログの改ざんを防ぎ、誰がカード会員データにアクセスしたか、どのようなセキュリティイベントがいつ発生したかなどを検出する機能を実現します。また、監査のために構成設定およびセキュリティ設定を監視し、コンプライアンスに従っていることを検証します。さらに、それらが変更された場合には、数秒以内に警告します。	✔	
要件11： システムおよびネットワークのセキュリティーを定期的にテスト	ファイル整合性監視機能は、変更を検知し、各変更をプログラム的に分析することで、変更が承認に値し、コンプライアンスにかなったものあるかを判断します。顧客固有のポリシーやプロセスにも適用できます。検知された変更がポリシーテストの失敗を引き起こした場合、自動的に修復し、システムを安全でコンプライアンスに準拠した状態に戻します。	✔	*
目的6：	**情報セキュリティポリシーの整備**		
要件12： 組織のポリシーとプログラムによる情報セキュリティのサポート	ポリシー順守（基準を満たした使用、システムの構成設定、および変更管理イベント）の証跡提出をサポートします。重要なシステムに対する予期せぬ変更を発見するだけでなく、監査に対応したレポートを提供、有効な手順や慣行のコンプライアンスを証明することができます。	✔	

*Tripwire IP360 は侵入テストは行いませんが、悪用の可能性がある脆弱性の発見や、スキャンによる修復の検証を支援します。

FORTRA™

Fortra.com

Fortraについて

Fortra は、他に類を見ないサイバーセキュリティ企業です。私たちはお客様のために、よりシンプルで強力な未来を創造します。当社の信頼できるエキスパートと統合されたスケーラブルソリューションは、世界中の組織にバランスとコントロールをもたらします。私たちはポジティブ・チェンジメーカーであり、サイバーセキュリティの旅路のあらゆる段階において、お客様の味方となります。詳細については、fortra.com をご覧ください。

　