White paper

Tripwireを活用したPCI DSS基準の遵守

※本ソリューション概要は米国Tripwire, Inc.によるホワイトペーパー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。

© 2008 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other marks are property of their respective owners. All rights reserved.

概要

Visaが打ち出した大規模な広告では「Visaカードはどこでも使える」という謳い文句を使っています。残念ながら、Visaの責任ではありませんが、大量のクレジットカードデータやその他の重要な情報が望ましくない場所に行き着いてしまっているのが現状です。クレジットカードデータの漏洩や損失事件の報告を聞かない日は1日もないほどで、メディアや政府内では追加のデータ保護法案に対する要求が高まっています。

このような事件の結果、PCI DSSのコンプライアンスのプレッシャーが日々高まっています。コンプライアンスはもはや選択の余地のない必須の義務であり、PCI DSSの要件を遵守できない場合には金銭的なペナルティや場合によってはクレジットカードトランザクションを引き受け/処理する権利の停止や取り消しのような事態に陥ることも考えられます。幸いなことに、PCI DSSのような基準が推奨するベストプラクティスを実行することによってITシステム、ハードウェア、およびデータをセキュアに保ち、顧客からの信頼や企業の評判の失墜を防ぐことができます。

Tripwireでは長年にわたって企業の皆様のITシステムの監視/管理、内部や外部からの攻撃やシステム変更や人的なエラーによる予期せぬ影響からハードウェア、ネットワーク、データベース、およびデータの保護をお手伝いしてきました。企業の皆様のPCI DSS要件の遵守をお手伝いすることは我々の長年の経験から言って当然の帰結と言えます。実際、Tripwire® Enterpriseでは多くの複雑なPCI DSS要件を何の手間もかけることなく満たすことができます。 Tripwire Enterpriseを活用することによって、継続的に情報を収集してPCI DSSコンプライアンスに必要なレポートや証拠を提出し、監査にかかる手間を省くことが可能になります。

コンプライアンスにとどまらない利点

企業の皆様の現在のフォーカスはPCI DSS監査に合格することにあるかもしれませんが、Tripwire Enterpriseではセキュリティ上のベストプラクティスの実行を手助けすることによって、ファイル完全性監視、ファイアウォール/ルータセキュリティコンプライアンス監視、およびIT構成コントロールなどの機能を通じてお客様のネットワークやデバイスを保護します。Tripwire Enterpriseではユーザが指定した監視対象において重要な構成ファイルなどの重要な項目への変更やその他の重要なシステム変更があった場合指定したユーザにアラートを発します。この結果、計画的に統制の行き届いた方法でシステム/アプリケーションセキュリティ、システムアップタイムの向上、顧客データの保護を実現できます。Tripwire Enterpriseではすべての完全性チェックや検知された違反の記録を保管し、監査、調査、履歴参照などで利用することが可能になり、コンプライアンスの証明に必要な情報が簡単に取得できます。これによって、監査に費やすITリソースを節約し、戦略的に重要な業務に時間を使うことができます。

© 2008 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other marks are property of their respective owners. All rights reserved.

コンプライアンス要求の高まり

複数の大手クレジットカード会社が協力し、重要なカード保持者のアカウントデータを盗難や詐欺から保護するためにPCI DSSが作成されました。PCI DSSの作成にはAmerican Express, Discover Financial Services, JCB, MasterCard WorldwideおよびVisa Internationalなどの企業が参加しました。最近では、Visaが2007年8月までに全ての加盟店のコンプライアンスを遵守している加盟店銀行に向けた金銭的なインセンティブを提供するなどコンプライアンスを促進する動きがさらに高まりを見せています。しかし、このようなインセンティブによってもコンプライアンスが達成できなかった場合、Visaは2007年12月31日を過ぎてもコンプライアンスが達成できていない加盟店に対して$25,000の罰金を科す意志を表明しています。このような罰金が発生した場合、おそらく加盟店がこれを負担することになると思われます。指定された時間内にコンプライアンスを達成できない加盟店がある場合、加盟店銀行はこのような支店に対してクレジットカードサポートの提供を中止するものと思われています。

カード業界データセキュリティ基準:PCI DSS

カード業界データセキュリティ協議会（www.pcisecuritystandards.org)はPCI DSSによって開発されたカード保持者データセキュリティ基準の採用を促進するために設立された非営利団体です。このセキュリティ基準は6つの主要なグループに分類されます。各グループには特定の要求が含まれます。これらの主要なグループでは、サービスプロバイダ、加盟店銀行に下記を要求しています:

グループ1: セキュアなネットワークの構築と維持

要求1: ファイアウォールを構築、維持し、適切なアクセス権限を提供することによって、重要なカード保持者データを不正アクセスから保護する。

要求2: ファイアウォールベンダーが提供するパスワード、その他のセキュリティ関連の初期設定を必ず変更する。

グループ2: カード保持者データの保護

要求3: 保存されている重要なカード保持者データがアクシデントまたは悪意をもってアクセス、乱用されないようにする。

要求4: 公開ネットワーク上でカード保持者データを送信する前には必ず暗号化する。

グループ3: 脆弱性管理プログラムの維持

要求5: アンチウィルスソフトウェアをインストールして、全ての脆弱性のあるハードウェア上で最新のアンチウィルス定義を維持する。

要求6: システム、アプリケーションに最新のセキュリティパッチを適用する。

© 2008 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other marks are property of their respective owners. All rights reserved.

グループ4: 強固なアクセス制御手段の実施

要求7: 重要なカード保持者データへのアクセスを組織内で職務上必要のある要員だけに提供する。
要求8: コンピュータへのアクセス権限を持つ各要員にユニークかつ追跡可能なIDを割り当てる。
要求9: 重要なデータを物理的ロケーションまたは職務の遂行上そのデータが必要な要員だけがアクセス可能な特定のマシン上に保存することによって、カード保持者データへのアクセスを制限する。

グループ5: ネットワークの定期的な監視とテスト

要件10: 誰がネットワークリソース及びカード保持者データにアクセスしたかを記録する。
要件11: セキュリティシステムとプロセスを定期的にテストして脆弱性、違反を発見する。

グループ6: 情報セキュリティポリシーの維持

要件12: 情報セキュリティの全ての側面をカバーする最新のポリシーを保持する。

加盟店銀行、サービスプロバイダがこのような基準を満たしている場合、監査基準を満たしているだけではなく、顧客のデータセキュリティを強化し、不適切なネットワーク、データセキュリティプラクティスによって生じた問題を解決するために時間を費やす必要のない情報システムを備えていることになります。PCI DSSのコンプライアンスは非常に道理にかなっているといえます。
このホワイトペーパーを読むことで、PCI DSSと同時にTripwire Enterpriseを利用したコンプライアンスの達成方法を学び、経営の効率性の向上、コスト削減、生産性の高い業務へのリソースの投資が可能になります。

© 2008 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other marks are property of their respective owners. All rights reserved.

Tripwire Enterpriseによる要件の遵守

PCI DSSの要件はシンプルな検査、検証アクティビティから継続的な監視を通じたコンプライアンスの保証まで多岐にわたります。Tripwire Enterpriseでは3通りの方法でこのような要求に対応します:

	カテゴリー	詳細	例
	**アウトオブザボックス**	Tripwire Enterprise **では内蔵される構成分析テストによってアウトオブザボックスで要求の遵守を助けます。**	**ゲストアカウントが無効になっているかどうかのテスト**
	**Tripwire Enterprise 7 及びプロフェッショナルサービス**	Tripwire Enterprise **ではプロフェッショナルなサービスによって構成分析テストにおいて顧客独自のニーズを満たすことで要求の遵守を助けます。**	**特定のホストだけがＤＭＺと通信できるかどうかのテスト**
	**証拠提出**	Tripwire Enterprise **では監査証跡を作成して、必要なプロセスが適切に遵守されていることを証明します。**	**システムに変更が加えられた場合、下記のような必要な手順を踏んで行われたという証拠を提供**: 1. **変更要求の提出** 2. **作業の実行** 3. **変更要求のクローズ**

下記の図を検証することで、どのようにTripwire Enterpriseを利用してコンプライアンスが達成できるかが分かります。カテゴリー列ではTripwireが各要求にどのように対応するかを図で示しています。

グループ1: セキュアなネットワークの構築と維持

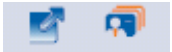
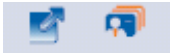
要求1: ファイアウォールを構築、保守し、適切なアクセス権限を提供することによって、重要なカード保持者データを不正アクセスから保護する。

ファイアウォールとは企業ネットワークに出入りするコンピュータトラフィック及び企業の内部ネットワーク内の重要なエリアへのトラフィックをコントロールするためのコンピュータデバイスです。ファイアウォールでは全てのトラフィックを検証して特定のセキュリティ基準を満たさないトラフィックをブロックします。

全てのシステムはインターネットからの不正なアクセスから保護される必要があります。よくあるのはインターネットからの一見重要でなさそうなパスによって、キーシステムへの保護されないパスが提供される、というパターンです。ファイアウォールは全てのコンピュータネットワークにとってキーとなる保護メカニズムなのです。

© 2008 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other marks are property of their respective owners. All rights reserved.

Tripwire Enterpriseではファイアウォール、ルータの状態を監視して、設定ファイル、ルールセット、OSへの許可されない変更を検知、レポートします。また、Tripwireではデバイスを以前の承認された状態にリストア（ロールバック）し、疑わしい設定のコピーを保持して分析を行い、必要があれば再導入（ロールフォワード）します。コンプライアンスを保証するためのタスクの多くを自動化し、自動的にこのようなアクティビティのレコードを生成することで、PCI DSS監査用の証拠提出が簡単に行えます。

要件	カテゴリ
1.1 下記を含むファイアウォール設定基準を設定:	
1.1.1 承認及び、全ての外部ネットワーク接続及びファイアウォールへの変更のテストの公式なプロセス	
1.1.8 ファイアウォール、ルータルールセットの四半期に１度の検証	
1.2 カード保持者データ環境に必要なプロトコル以外の'信頼できない'ネットワーク、ホストからの全てのトラフィックを拒否するファイアウォールの構築:	
ウェブプロトコル - HTTP (**ポート** 80) **及び**(SSL) (**通常ポート** 443).	
システム管理プロトコル(例：SSH **もしくは** VPN).	
その他ビジネスで必要なプロトコル(例：ISO 8583 **で必要なプロトコル**)	
1.3 公開されておりアクセス可能なサーバと、ワイヤレスネットワークからの接続を含むカード保持者データを保存するシステムコンポーネント間での接続を制限するファイアウォールの構築。ファイアウォール構成には下記のようなものが含まれる必要があります:	
1.3.1 DMZ **内の** IP **アドレスへのインバウンドインターネットトラフィックの制限。**	
1.3.2 内部アドレスのインターネットから DMZ **への通過の禁止**	
1.3.3 動的パケットフィルタリングの実施("設定済みの"接続だけがネットワーク内に許可される)	
1.3.4 データベースを DMZ **から隔離された内部ネットワークゾーンに配置**	
1.3.5 カード保持者データ環境にとって必要なアウトバウンドトラフィックの制限	

© 2008 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other marks are property of their respective owners. All rights reserved.

1.3.6 ルータ設定ファイルの保護、同期化。例えば、実行中の設定ファイル(ルータの通常機能用)とスタートアップ設定ファイル(マシン再起同時の)には同じセキュアな設定を使用する。	
1.3.7 特別許可されていない全てのインバウンド、アウトバウンドトラフィックの拒否	
1.3.8 ワイヤレスネットワークとカード保持者データ環境間での周辺ファイアウォールのインストール、このようなファイアウォールを設定してワイヤレス環境からのトラフィックを拒否するように設定.	
1.3.9 企業内のネットワークへのアクセスに使用されるインターネットに直接接続可能なモバイルコンピュータ、従業員所有のコンピュータ上でパーソナルファイアウォールをインストール	
1.4 外部ネットワークとカード保持者データをシステムコンポーネント間でのパブリックアクセスの禁止	
1.4.1 DMZ を実装して全てのトラフィックをフィルタリング、スクリーニングし、インバウンド、アウトバウンドインターネットトラフィックの直接ルートを禁止	
1.4.2 カードアプリケーションから DMZ 内の IP アドレスへのアウトバウンドトラフィックを制限	
1.5 IP マスカレーディングを実施して、内部アドレスを変換してインターネット上で公開するのを禁止します。ポートアドレス変換(PAC)やネットワークアドレス変換(NAT)のような RFC 1918 アドレススペースを実装する技術を使用してください。	

要求2: ファイアウォールベンダーが提供するパスワード、その他のセキュリティ関連の初期設定を必ず変更する。

ハッカー (企業内部/外部の)はしばしばベンダー提供のデフォルトパスワード設定を使用して、システムへの侵入を試みます。このようなパスワードや設定はハッカーのコミュニティではよく知られており、公開されている情報からも簡単に判断することができます。

Tripwire Enterpriseではネットワークシステム、デバイスがCISやPCI DSSのような広く認識されたソースによって作成された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します。Tripwireは継続的な監視、検知を通じてコンプライアンス違反の状態にあるシステム、デバイスを明確化し、危険な設定に関するアラートを出し、明確化されたコンプライアンス上の問題の修正作業に関する進行状況を追跡し、コンプライアンスの維持を保証します。

© 2008 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other marks are property of their respective owners. All rights reserved.

Tripwire では企業システム、データの保護に長い歴史を誇っており、PCI DSS のような重要な業界標準とのコンプライアンスの保証も信頼して任せることができます。

要件	カテゴリ
2.1 ネットワーク上でシステムをインストールする前には常にベンダー提供時の初期設定を変更する（例：パスワード、ＳＮＭＰコミュニティストリングを含む、必要ないアカウントは削除する、など）	
2.1.1 ワイヤレス環境の場合，ＷＥＰキー、デフォルト SSID、パスワード、SNMP コミュニティストリングのようなワイヤレスベンダーが提供する初期設定を変更する。SSID ブロードキャストを無効にする。Wi-Fi 保護アクセス(WPA や WPA2)技術を有効にして暗号化や認証を行う。	
2.2 全システムコンポーネントの設定基準を確立する。 このような基準によって全ての既知のセキュリティ脆弱性に対処ができており、SANS,NIST,CIS のような業界に広く受け入れられたシステム強化基準と一致していることを確認する。	
2.2.1 １台のサーバにつき１つの主要な機能のみを実装する。 *（例：ウェブサーバ、データベースサーバ、DNS は別々のサーバ上で実装する。）*	
2.2.2 不必要で安全でない全てのサービス、プロトコルを無効にする。*（サービスやプロトコルはデバイス特有の機能の実行時には直接必要ありません。）*	
2.2.3 システムセキュリティパラメータを設定して濫用を防止する。	
2.2.4 スクリプト、ドライバ、サブシステム、ファイルシステム、必要ないウェブサーバのような全ての必要ない機能を削除する。	
2.3 全ての非管理コンソール管理アクセスを暗号化する。 ウェブベースの管理アクセス、その他の非コンソール管理アクセスでは SSH，VPN，または SSL/TLS のような技術を使用してください。	

グループ2: カード保持者データの保護

要求3: 保存されている重要なカード保持者データがアクシデントまたは悪意をもってアクセス、乱用されないようにする。

暗号化はカード保持者データ保護の重要な一部です。侵入者がその他のネットワークセキュリティ統制をかいくぐり、適切な暗号化キーなしに暗号化されたデータへのアクセス権限を得た場合、データはその人物にとっては読み取り、使用することが不可能です。リスク緩和の手段として保存したデータのその他の有効な保護方法も考慮されるべきです。例えば、リスク緩和の手段としては、絶対に必要でない限りカード保持者のデータを保存しない、カード保持者のデータを切り詰める、暗号化されていない電子メールでPANを送信しない、といったものがあります。

© 2008 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other marks are property of their respective owners. All rights reserved.

Tripwire Enterprise では特定のデータタイプ（カード保持者データのような）が保存される前に削除されたことを証明し、必要であればこのプロセスを自動化します。Tripwire ではまた、誰かがファイル内の暗号化キーを修正または取り替えた場合、そのような問題が解決するまで追跡します。

要件	カテゴリ
3.1 カード保持者情報記録を最小限にとどめる。データ保存、処分ポリシーを制定する。ストレージの量、保存期間をデータ保存ポリシーにおいて文書化されている通り業務上、法律上、規制上の目的で必要な程度に制限する。	
3.5.1 キーへのアクセスを必要最小限の管理者に制限する。	
3.5.2 キーを最小のロケーションに最小の形式でセキュアに保管する。	
3.6.3 キーストレージを保護する。	
3.6.4 定期的にキーを変更する。 **• アプリケーションにおいて必要と認められる、推奨される期間ごとに。自動的に行うのが望ましい。** **• 少なくとも年に１回。**	
3.6.5 古いキーを破棄する。	
3.6.7 無許可のキー交換の防止。	
3.6.8 既知のキーまたは安全でない疑いのあるキーを交換する。	

© 2008 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other marks are property of their respective owners. All rights reserved.

要求4: 公開ネットワーク上でカード保持者データを送信する前には必ず暗号化する。

ハッカーが容易に情報をインターセプト、変更できるようなネットワーク上で重要な情報を送信する場合、暗号化する。

Tripwire Enterprise では設定ファイルの必要なセキュリティ設定を検索し、定義したポリシーからの逸脱があった場合アラートを出します。設定ファイルのコンプライアンスが保証されると、Tripwire は変更の監視、アラートを行い、変更の検証を可能にします。Tripwire では全ての監視アクティビティを記録、報告しますので、監査に関して継続中の監視の証拠の提出が容易なタスクになります。

要件	カテゴリ
4.1 SSL**や**TLS,IPSEC**のような強固な暗号化技術を使用して公開ネットワーク上の重要なカード保持者データを保護する。** PCI DSS **における公開ネットワークの例としてはインターネット、**Wi-Fi (IEEE 802.11x), GSM, GPRS **などがあげられます。**	
4.1.1 ワイヤレスネットワークでカード保持者データを送信する場合、 Wi-Fi**保護アクセス**(WPA**もしくは**WPA2), IPSEC VPN, **または**SSL/TLS**のような技術を使用して送信データを保護する。情報の機密性、ワイヤレス**LAN**へのアクセスを保護する場合、**WEP**だけに依存しない。**WEP**が使用されている場合、下記を実施する**: • **最低でも**104**ビットの暗号化キーと**24**ビット初期化値とともに使用する。** • Wi-Fi**保護アクセス**(WPA**または**WPA2)**技術、**VPN, **または**SSL/TLS**などと併用する。** • **四半期に１回共有**WEP**キーをローテーションさせる。(技術的に可能であれば、自動的に行う**) **•共有**WEP**キーにアクセス権限を持つ要員に変更があった場合、キーをローテーションさせる。** • MAC **アドレスに基づいてアクセスを制限する。**	

© 2008 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other marks are property of their respective owners. All rights reserved.

グループ3: 脆弱性管理プログラムの維持

要求5: アンチウィルスソフトウェアをインストールして、全ての脆弱性のあるハードウェア上で最新のアンチウィルス定義を維持する。

多くの脆弱性や悪質なウィルスが企業の電子メールを通じて企業ネットワークに侵入します。全ての電子メールシステム及びデスクトップ上でアンチウィルスソフトウェアを使用してシステムを悪質なソフトウェアから保護してください。

Tripwire Enterprise ではコンプライアンス違反の状態にあるシステムを検知し、アップデートが行われない場合アラートを発します。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。このアプローチによってパターンマッチング、ウィルス定義に依存するアンチウィルスソフトウェアが補完されます。Tripwire ではシステム変更を追跡、報告しますので、ゼロデイ攻撃が発生した場合、ウィルス定義が有効になる前に被害を受けたシステムを検知します。検疫を目的とし、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、修復プロセスの短縮、簡略化が可能になります。

要件	カテゴリ
5.1 ウィルスに影響を受ける全システム上でアンチウィルスシステムを導入する(特に PC及びサーバ)。 ***注釈: ウィルスに影響を受けるシステムには基本的にUNIX ベースのOS,メインフレームは含まれません。***	

要求6: システム、アプリケーションに最新のセキュリティパッチを適用する。

悪意のある人物はセキュリティ上の脆弱性を使用してシステムへのアクセス権限を得る場合があります。このような脆弱性の多くはベンダーによって提供されるセキュリティパッチによって修正されます。全てのシステムには最近リリースされた適切なソフトウェアパッチを適用して、従業員、外部ハッカー、ウィルスによる脆弱性の利用から保護する必要があります。注釈: 適切なソフトウェアパッチとは十分に評価、テストされ、既存のセキュリティ設定と矛盾しないことが確認されているものを意味します。社内開発アプリケーションに関しては、標準的なシステム開発プロセスとセキュアなコーディング技術を使用することによって、多くの脆弱性は回避できます。

© 2008 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other marks are property of their respective owners. All rights reserved.

Tripwire Enterprise ではセキュリティパッチが適切にターゲットシステムに導入されているかどうか確認し、パッチが正しく適用されていないシステムを明確化します。Tripwire では適切なパッチが行われているかどうかの検証が可能ですので、Tripwire をパッチ導入プロセスの一部として使用することによって、パッチの適用に失敗した場合のリスク、影響を軽減し、適切なパッチ導入の確認として独立した監査証跡を生成します。

要件	カテゴリ
6.1 全システムコンポーネントとソフトウェアにベンダー提供の最新のセキュリティパッチがインストールされていることを確認する。セキュリティパッチはリリースから１ヶ月以内にインストールする。	
6.3.1 導入前に全てのセキュリティパッチ、システム、ソフトウェア設定変更をテストする。	
6.3.5 本番システムが稼働する前にテストデータとアカウントを削除する。	
6.3.6 アプリケーションが稼働して顧客にリリースされる前にカスタムアプリケーションアカウント、ユーザ名、パスワードを削除する。	
6.4 システム、ソフトウェア設定変更時には変更管理手順に従う。このような手順には下記のようなものが含まれる必要がある:	
6.5.8 セキュアでないストレージ	
6.5.10 セキュアでない構成管理	

© 2008 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other marks are property of their respective owners. All rights reserved.

グループ4: 強固なアクセス制御手段の実施

要求7: 重要なカード保持者データへのアクセスを組織内で職務上必要のある要員だけに提供する。
これによって、重要なデータには承認された者しかアクセスできないことが保証されます。
多くの企業はデータ保護に関するポリシーは有していますが、変更によって知らず知らずのうちにその保護に悪影響が出た場合の検知メカニズムは持っていません。Tripwire Enterprise では重要なデータへのアクセスが知る必要のある要員だけに与えられていること、特定の期間に統制がきちんと実施されていたことを保証します。 このような証拠を提供することによって、企業は高いコストのかかるテストや監査中の統制の検証を回避することができます。

要件	カテゴリ
7.1 カード保持者情報やコンピュータ資源へのアクセスは職務上アクセスが必要な要員だけに制限する。	
7.2 複数のユーザが存在するシステムにおいては、知る必要のある要員だけにアクセスを制限し、アクセスを許可されていない場合は全て拒否するよう設定されたメカニズムを確立する。	

要求8: コンピュータへのアクセス権限を持つ各要員にユニークかつ追跡可能なIDを割り当てる。
各要員にユニークなIDを割り当てることによって、重要なデータやシステム上でのアクションの実行は既知の承認されたユーザによって行われ、アクションを実行したユーザを追跡することが可能になります。

Tripwire Enterprise では新規ユーザ ID や既存のユーザ ID の変更、削除を検知し、適切なシステムアクセス制御が実施されていることを証明できます。

要件	カテゴリ
8.5.1 ユーザ ID、認証情報、その他の識別用オブジェクトの追加、削除、変更を統制する。	
8.5.4 契約が終了したユーザのアクセスは直ちに取り消す。	
8.5.5 少なくとも90日ごとにアクティブでないユーザアカウントを削除する。	
8.5.6 ベンダーがリモート保守で使用するアカウントは必要な期間中のみ有効にする。	
8.5.9 ユーザパスワードを少なくとも90日に1回は変更する。	
8.5.10 パスワードの長さには少なくとも7文字以上を要求する。	
8.5.11 アルファベットと数字の両方を含むパスワードを使用する。	

© 2008 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other marks are property of their respective owners. All rights reserved.

8.5.12 過去4つのパスワードのいずれか1つと同じパスワードの使用を許可しない。	
8.5.13 6回以上ログインアクセス試行があった場合、ユーザIDをロックアウトして反復アクセスを制限する。	
8.5.14 ロックアウト機関を30分もしくは管理者がユーザIDを有効にするまでに設定する。	
8.5.15 セッションが15分以上休止状態にある場合、ユーザに再度パスワードを入力して端末を有効にするように要求する。	
8.5.16 カード保持者情報を含む全てのデータベースへの全アクセスを認証する。これには、アプリケーション、管理者、その他全てのユーザによるアクセスが含まれます。	

グループ5: 定期的なネットワークの監視とテスト

要件10: 誰がネットワークリソース及びカード保持者データにアクセスしたかを記録する。

ログメカニズムやユーザアクティビティを追跡できる機能は非常に重要です。全ての環境でログが存在することで、エラーがあった場合に綿密な追跡、分析が可能になります。システムアクティビティログがないとエラーの原因の究明は非常に困難です。

Tripwire Enterpriseではシステム変更と変更を担当する個別のユーザアカウントと関連付けし、この情報を変更や削除が不可能なTripwireレポートファイル内に記録します。さらに、Tripwireではシステム設定を、ベースライン、基準と比較することによってテストし、統制が適切でない部分または統制が存在しない部分を明確化します。

要件	カテゴリ
10.1 システムコンポーネント（特に管理者権限によってされたアクセス）への全アクセスを個々のユーザにリンクするプロセスとして確立する。	
10.2.7 システムレベルオブジェクトの作成、削除。	
10.4 全ての重要なシステム時計、時間の同期化。	
10.5 監査証跡を保護して、変更できないようにする。	
10.5.1 監査証跡の閲覧を職務上必要な要員だけに制限する。	
10.5.2 監査証跡を不正な変更から保護する。	

© 2008 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other marks are property of their respective owners. All rights reserved.

10.5.3 監査証跡ファイルを集中ログサーバもしくは変更できないメディアに速やかにバックアップする。	
10.5.4 ワイヤレスネットワークのログを内部LAN上のログサーバ上にコピーする。	
10.5.5 ログ上でファイル整合性監視、変更検知ソフトウェアを使用して、既存のログデータがアラートなしで変更できないようにする（ただ、追加される新しいデータにはアラートの必要はない）。	
10.6 全システムコンポーネントのログを毎日検証する。ログの検証には、IDSのようなセキュリティ機能を実行するサーバ、認証（AAA）サーバを含んでください。	

要件11: セキュリティシステムとプロセスを定期的にテストして脆弱性、違反を発見する。

脆弱性は常にハッカーや研究者によって発見され続け、新しいソフトウェア、システム、カスタムソフトウェアによって新しい脆弱性が絶えず生み出されていますので、頻繁にテストを行って、常に万全のセキュリティ状態が維持されているかどうか確認してください。

Tripwire Enterpriseでは企業全体のファイル整合性を監視します。また、強固かつフレキシブルなレポートや、事前定義されたルールセットを提供し、OSをインテリジェントにカバーします。Tripwireは変更管理プロセスの一部として企業管理システムに統合され、誰かが本番システム用にデザインされたセキュリティシステム、プロセスをかいくぐった場合、検知します。このような検知によって、このような不正なアクティビティによって生み出される問題への対応、セキュリティテストの管理の向上が可能になります。

要件	カテゴリ
11.3 少なくとも 1 年に 1 回または重要なインフラ、アプリケーションアップグレード、変更（例：OS アップグレード、環境にサブネットワークを追加、環境にウェブサーバを追加）があった後は侵入テストを実施してください。 このような侵入テストには下記が含まれている必要があります:	
11.4 ネットワーク侵入検知システム、ホストベース侵入検知システム、侵入防止システムを使用して、全てのネットワークトラフィックを監視し、疑わしい事象については適切な要員にアラートを出す。全ての侵入検知、侵入防止エンジンを最新に保っておいてください。	

© 2008 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other marks are property of their respective owners. All rights reserved.

11.5 ファイル整合性監視ソフトウェアを導入して、重要なシステム、コンテンツファイルの無許可の変更があった場合、適切な要員にアラートを出し、このようなソフトウェアで重要なファイル比較を少なくとも週1回は実行するようにしてください。 ***重要なファイルは必ずしもカード保持者データを含むものだけとは限りません。ファイル整合性監視上の目的においては、重要なファイルとは通常変更されないけれど、変更された場合システムに脆弱性が生まれるようなファイルを意味します。ファイル整合性監視製品は通常、関連OSの重要なファイルによって事前設定されています。カスタムアプリケーションのファイルのようなその他の重要なファイルはサービスプロバイダ本人が評価、定義する必要があります。***	

グループ6: 情報セキュリティポリシーの維持

要件12: 情報セキュリティの全ての側面をカバーする最新のポリシーを保持する。

強固なセキュリティポリシーによって企業全体のセキュリティの雰囲気が決まり、従業員に対して何が期待されるのか、が通知されます。全ての従業員はデータの重要性及びデータ保護の責任に関して認識する必要があります。

Tripwire Enterpriseではガバナンスに関する文書を作成するのではなく、手順を守っていることの証明を助けます。ポリシー違反があった場合、Tripwireはその違反の証拠を提供します。

要件	カテゴリ
12.1.3 少なくとも 1 年に 1 回は検証を行い、環境が変更した場合、アップデートを実行する。	
12.5.2 セキュリティアラート、情報を監視、分析し、適切な要員に配布する。	
12.9.2 少なくとも年に1回はプランのテストを実施する。	
12.9.5 侵入検知、侵入防止、ファイル整合性監視システムのアラートを含む。	

© 2008 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other marks are property of their respective owners. All rights reserved.

経験豊富な企業が提供する定評あるソリューション

サーバ、ネットワークデバイスへのたった1つの小さな変更によって、企業システムネットワーク全体に大打撃を受けてしまう可能性もありますので、ITではシステム、デバイス変更が望ましいものかどうかを検知、報告、評価する手段が必要です。Tripwire Enterpriseによって企業は重要なファイルの監視、このようなファイルと業界基準や内部ポリシーとの比較、承認されていない変更の検知、無許可の変更があった場合の適切な要員へのアラートによってセキュリティ脆弱性の減少、データ保護を実現することができます。さらに、Tripwireでは実施されているセキュリティ統制の証拠を提供しますので、PCI DSSのような基準の遵守が非常に簡単なタスクとなります。

Tripwireによって、企業は下記のような強固なビジネスベストプラクティスを実現することが可能になります:

・ リスク軽減、コスト削減によるコンプライアンス、セキュリティ対応;
・ 変更管理、構成自動化を通じた予定外の作業の減少;
・ ダウンタイムの削減、迅速なリカバリによるシステム可用性の向上
・ 構成管理データベース(CMDB)、 ITサービス管理(ITSM), 及びITインフラライブラリ(ITIL)プロジェクトにおける投資対効果の向上

Tripwireでは、長年のソリューション設計、顧客とのコンサルティングで得た経験を通じて、監視するシステムや顧客が使用する多くのアプリケーション用の包括的なルールセットを作成しました。Tripwireにより、PCI DSSコンプライアンスの達成、よりセキュアな企業ITインフラを実現いただくことが可能です。

【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。

© 2008 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All other marks are property of their respective owners. All rights reserved.