White paper

PCI DSS

- PCI データセキュリティ基準

※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、「PCI DSS」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。

概要

Visaによる大規模な広告キャンペーンではVisaのカードは「行きたい場所どこでも使える」と謳っています。残念ながら(Visaに非はありませんが)、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「行って欲しくない場所」に行き着いてしまっているのが現状です。重要なクレジットカードが漏洩したり、なくなってしまったりというニュースを聞かない日は1日もないほどです。ワシントンポスト紙では2005年を「情報漏洩の1年」と呼んだほどです。

このような事件が起きるとほとんどの場合、メディアや政府内で追加のデータ保護法令の必要性が叫ばれます。マサチューセッツ州の下院議員エドワード・マーキー氏はCardSystems社で発生した情報漏洩(4,000万件のクレジットカードデータが盗難された)事件を「アメリカの消費者を保護するための新しい連邦法案の必要性を浮き彫りにする事件」であるとしています。

相次ぐ情報漏洩、データ流出に対して被害にあったある企業のCISOは「介入もいいが、法案作成に関して一番難しいのはデータ漏洩がどこから発生するか分からず、予測が非常に難しいという点です」と語っています。

ただし、Visaではこのような最近の情報漏洩事件や法案に対する要求が高まる前からVisaの支払いやカードデータを処理するすべての加盟店とサービスプロバイダに適用されるCISP（カード所有者情報セキュリティプログラム）と呼ばれる私的なセキュリティ基準を作成していました。このプログラムは2001年に開始されましたが、最近になってVisa、American Express, Diner's Club, Discover, JCBおよびMasterCardの協力によりCISPに基づいた新しい基準PCI DSS（決済カード業界データセキュリティ基準）が作成されました。2005年6月30日時点で決済カードに関する情報を処理、送信、保存するすべての加盟店、サービスプロバイダはこのPCIの遵守を要求されました。

2006年9月にPCIセキュリティ基準審議会はPCIデータセキュリティ基準v1.1を発表しました。この文書ではPCIの基本的な要件について説明されており、プログラムの管理および技術的な側面に焦点が当てられています。あわせて当該基準の検証要求とコンプライアンス違反があった場合の制裁の可能性についても見直されています。

PCI DSSの基本情報:コンプライアンス対象企業、コンプライアンス要求、検証要求、制裁

コンプライアンス要求、検証要求の細部について検証する前に、PCI DSSの基本情報を把握しておくことは非常に重要です。まず、PCI DSSは法律ではないということを把握しておくことは重要なポイントです。PCI DSSはメンバー、加盟店、およびサービスプロバイダがクレジットカード会社との契約に従って遵守する必要のある私的なセキュリティ基準です。PCI DSSは法律ではありませんが、クレジットカード会社はクレジットカードのトランザクションを引き受け、処理する権利といった契約上のペナルティや制裁を通じてPCIを施行できます。

PCI DSSはカード保持者データを保存、処理、送信するすべてのメンバー、加盟店、およびサービスプロバイダに適用されます。PCIは「カード保持者のデータ環境に含まれ、接続されるすべてのネットワークコンポーネント、サーバ、アプリケーション」と定義されるすべての「システムコンポーネント」に適用されます。

PCI DSSコンプライアンスを要求する各クレジットカード企業間で詳細に小さな差異はありますが、PCI DSSは6つの主目的に沿って設定された12の個別のコンプライアンス要求（この要求のそれぞれにより詳細なコンプライアンスステップが含まれます）で構成されます。

この6つの主目的を達成することによって、クレジットカード番号やその他の重要なカード保持者データを損失や漏洩から保護するための包括的な情報セキュリティシステムの構築を目指します。

コンプライアンス要求以外にも、PCI DSSでは検証要求も含まれます。このような要求はクレジットカード会社によって若干の違いはありますが、最も包括的な要求（VisaとMasterCard）では検証に関して次の3つのレベルを設定しています。

(1) オンサイトセキュリティ監査
(2) 自己評価用の問診表
(3) ネットワークスキャン

要求される検証レベル、検証作業の頻度はPCI DSSの適用対象となる加盟店、サービスプロバイダに割り当てられるレーティングによって変わります。このレーティングはリスク、トランザクション/アカウントボリュームに基づいて決定されます。

最後に、PCI DSSプログラムではコンプライアンス違反があった場合の金銭的なペナルティやその他の契約上の制裁に関しても明記しています。例えば、Visa PCIプログラムでは、PCI DSSコンプライアンスに違反する加盟店やサービスプロバイダでデータ漏洩事件が発生した場合、メンバーは事件1回につき$500,000までの罰金を課されることがあります。トランザクション情報の損失、盗難、もしくはその疑いがある場合にVisaに直ちに通知しないVisaメンバーは1回の事件につき$100,000の罰金、さらにPCI違反によってVisaとそのメンバーに対して即時に重大なリスクが発生する場合追加の罰金を課される可能性があります。

PCI DSSコンプライアンスを達成できない場合メンバーはクレジットカードトランザクションを引き受け、処理する権限を停止、もしくは取り消される場合もあります。もちろん、Solutionary社のChris Noel氏が語るように評判の低下や逸失利益もコンプライアンス達成のモチベーションとなります。「『申し訳ありませんお客様のデータが流出してしまいました。詐欺的なトランザクションがあった場合以下のフリーダイヤルにご連絡ください』というようなプレスリリースをだす加盟店にはなりたくありません。お客様の財務情報という最も重要な資産を守れなかったという事実は企業にとって大きなダメージとなります。」コンプライアンスを達成するにはこのような基本的な情報を理解しつつPCIの12のコンプライアンス要求を詳細に検証することが必要です。

コンプライアンス要求: データセキュリティ確保のための12のステップ

上記で述べたように、PCI DSSコンプライアンス要求は6つの主要なカテゴリに沿った12の要求から構成されています。グラム・リーチ・ブライリー法やHIPAAのようなITセキュリティに関する法律の多くは管理、技術、および物理要求に分類されますが、PCI DSSはこのような分類はされていません。

但し、本ホワイトペーパーではPCI DSSとこのような法律の要求を比較したい方のために、以下の表ではPCI DSSの12の要求を管理、物理、技術的な要素に分類しています。PCI DSSでは無数の詳細なサブ要求を含みますので、この表ではすべての要素の包括的なリストを掲載するよりもサンプル要素を使って各要求について説明します。PCI DSSは以下のように12の基本的な要求と対応するサブ要求から構成されます。

PCI DSS	
セキュアなネットワークの構築と維持	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。 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。
カード保持者データの保護	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。 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。
脆弱性管理プログラムの維持	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。 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。
強固なアクセス制御手段の実施	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。 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。 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。
ネットワークの定期的な監視およびテスト	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。 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。
情報セキュリティポリシーを維持	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。

検証要求: コンプライアンスの維持と証明

上記で述べたとおり、コンプライアンス要求の実施はプロセスのスタート地点に過ぎません。PCIでは企業が継続的にPCI基準を遵守し続けることを保証するために必要とされる一連の検証要求を定めています。以下の表ではPCI DSSの検証ステップについて説明しています。

レベル	検証アクション	検証担当者	期限
1	年1回のオンサイトPCIデータセキュリティ分析と四半期に1回のネットワークスキャン	資格を取得したセキュリティ分析担当者、もしくは当該企業が承認したスキャニングベンダーの役員が承認した場合は内部監査	2004年9月30日 新規レベル1加盟店の検証期限は1年以内です。
2	年1回のPCI自己評価用の問診表および四半期に1回のネットワークスキャン	加盟店 承認されたスキャニングベンダー	新規レベル2加盟店: 2007年9月30日
3	年1回のPCI自己評価用の問診表および四半期に1回のネットワークスキャン	加盟店 承認されたスキャニングベンダー	2005年6月30日
4	年1回のPCI自己評価用の問診表および四半期に1回のネットワークスキャン	加盟店 承認されたスキャニングベンダー	検証要件と検証日は当該加盟店の加盟店開拓会社によって決定されます。

レベルはボリュームやリスクなどの要素に基づいて決定されます。

レベル	詳細
加盟店レベル 1	カードによる取引数が年間 600 万件以上の加盟店（受け入れチャネルの種類は問わない）。 ハッカー行為または攻撃に起因するアカウント・データの侵害を受けた加盟店。 Visa システムに対するリスクを最小化するためのレベル 1 加盟店要件を満たしているものと Visa によって判断された加盟店。 Visa 以外のクレジット・カード・ブランドによってレベル 1 に分類された加盟店。
加盟店レベル 2	Visa カードによる取引数が年間 100 万～600 万件の加盟店（受け入れチャネルの種類は問わない）。
加盟店レベル 3	Visa カードによる E-コマース取引数が年間 2 万～100 万件のすべての加盟店。
加盟店レベル 4	Visa カードによる E-コマース取引数が年間 2 万件未満の加盟店、および Visa カードによる取引数が年間 100 万件未満のすべての加盟店（受け入れチャネルの種類は問わない）。
サービスプロバイダ1	すべての VisaNet プロセッサ(メンバーおよび非メンバー)およびすべてのペイメントゲートウェイ
サービスプロバイダ2	レベル1に属さず、年間1,000,000以上のVisaアカウント/トランザクションを保管、処理、送信するサービスプロバイダ
サービスプロバイダ 3	レベル 1 に属さず、年間 1,000,000 以下の Visa アカウント/トランザクションを保管、処理、送信するサービスプロバイダ

目標の達成: PCI DSSの実施

上記の表ではPCI DSS実施上の課題のほとんどは技術的/管理的側面にあることが明らかになりました。クレジットカードデータで発生するリスクのほとんどはセキュリティ上の技術面/管理面の脆弱性の悪用が原因であることを考えるとこれはそれほど驚くべきことではありません。

PCI DSSでセキュリティ上の対策の継続的な検証を求めている事実、セキュリティを悪用する技術は日々進歩しているという事実からPCI DSSのコンプライアンスを求められる企業はインストールするだけでよいソリューションを実施することなどできないことは明白です。

Visa USAの詐欺対策部門の上級副社長であるJohn Shaughnessy氏は「PCI DSSによってセキュリティ対策の基準が上がっており、コンプライアンスは継続的なプロセスになる」と語っています。但し、どのような万全のセキュリティ対策も全体的なビジネスプロセスと調整して企業内の社員や部門がセキュリティ保護対策を変更したり、ポリシーや手順を迂回しないことが保証されない限りうまく行きません。例えば、ハッカーによって4,000万のMasterCardクレジットカードアカウントが漏洩したことが明らかになった後、CardSystems社(このようなクレジットカードのプロセッサ) は影響を受けたデータのうち200,000件のデータはポリシーに違反して研究目的で使用する個別のデータベース内に保存されていたことを認めました。

さらに、企業は検証作業を、コンプライアンスを証明しコンプライアンスの監査の助けとなるような記録を保管することによって裏付ける必要があります。PCI DSSではログ、追跡、および監査可能な記録の提出に関して多数の要件を明記しています。PCI DSSではいつ、どのようにシステムやレコードに承認されない変更が行われたかを検知する手段の実施も要求しています。

PCI DSSの10.5.5では、既存のログデータが改ざんされた場合に必ずアラートが発せられるようにログに対してファイル完全性監視/変更検知ソフトウェアを使用するように要求しています。つまり、クレジットカード会社から承認を受けた独立監査人が年1回のオンサイト監査を実施する場合には企業は明確、包括的かつ信頼性の高い記録を提出してコンプライアンスを証明する準備ができている必要があるのです。

決済処理企業向けにセキュリティ監査を実施する某企業につとめるNigel Tranter氏は「罰金を課される企業も出てくるでしょうし、強制的な方法が適用される場合もあるでしょう」と予測しています。PCI DSSの課題に対応するためには、企業は技術的な方策、管理上のベストプラクティス、健全なIT意思決定を組み合わせて変更監査プログラムを作成する必要があります。PCI DSS要件が実施され、検証中にコンプライアンスを証明する信頼できる記録が存在し、すべての変更を追跡、証明できる状態を確保することによって、PCI DSSコンプライアンスを要求される企業は監査の時期がやってきても何も心配することはないのです。

+++

【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。