



PCI規格に対応する基盤の構築

チェック・ポイントのソリューションで実現するPCI 1.1への準拠

Contents

本書の内容

概要	3
PCI規格の概要	4
PCI規格の認定監査機関とスキャン・ベンダーの役割	9
米国と欧州の違い	9
PCI規格の課題	10
PCI規格に準拠するための検討項目	11
PCI規格の各要件に対応するチェック・ポイントのソリューション	12
まとめ	27
付録：PCI規格準拠に関するチェック・ポイント製品	28

概要

クレジット・カードなどのサービスを提供するのペイメント・カード大手各社は、MasterCardとVisaを中心として、カード取扱業者をカード会員情報の盗難や不正使用から保護することを目的に、Payment Card Industry (PCI) Data Security Standardと呼ばれる一連の共通データ・セキュリティ要件を導入しました。過去に存在していた複数の規格を統合したこのPCI規格は、カード会員情報を保管、処理、または送信するすべての事業者に適用されます。

PCI規格に準拠する必要がある企業(加盟店、銀行、サービス・プロバイダなど)は、そのレベルに応じて、四半期ごとのネットワーク・スキャン、自己診断、訪問調査といったさまざまな検証作業を実施することが求められます。例えば、電話、Web、郵便、または店舗での取引が年間600万件を超えるレベル1の加盟店は、四半期ごとのネットワーク・スキャンに加えて、第三者の認定監査機関による年1回の監査に合格する必要があります。

インターネット・セキュリティの分野で世界をリードするチェック・ポイントは、加盟店や金融機関、情報処理業者によるPCI規格の準拠を支援する一連のソリューションを提供しています。チェック・ポイントの各ソリューションは、包括的で統合された機能を提供し、PCI規格に準拠するための強固な基盤として機能するほか、それ以外のセキュリティ規格に共通する各種要件の遵守も支援します。加えて、リスクの軽減、新たな決済チャネル(Webベースのサービスなど)のサポート、およびカード会員やビジネス・パートナーの信頼性向上を実現することにより、ビジネス面でも大きなメリットをもたらします。

PCI規格の概要

クレジット・カード会社各社は、MasterCardとVisaを中心として、電子決済システムの完全性と信頼性を今後も維持していくために、Payment Card Industry (PCI) Data Security Standardと呼ばれる一連の共通セキュリティ要件を共同で策定しました。PCI規格の各要件は、加盟店、銀行、第三者の決済処理業者を、機密性の高いカード会員情報の盗難や不正利用から保護することを目的としています。

1996年以降、電子商取引が広く普及し、脅威が高度化・複雑化していったことに伴い、ペイメント・カードの会員情報は、盗難や不正利用の格好の標的となっています。この傾向は、インターネット接続、リモート・サイト接続、リモートPCやモバイル・デバイスによるアクセス、無線LANの導入などにより企業ネットワークの複雑化が進むことで、さらに拍車がかかっています。また、インターネットがペイメント・カードの決済チャネルとして用いられるようになったことや、ハッカーの手法がますます洗練されてきていることを背景に、なりすましによるカード詐欺の危険性も高まっています。そのため、これらの不正利用や詐欺行為を広い範囲で防止することが目下の課題となっています。米連邦取引委員会によれば、何らかの形で個人情報盗難の被害を受けている米国人は、年間1,000万人にも上ります。

最近発生している多くの有名なセキュリティ侵害事件は、データ・セキュリティを強固にすることの重要性を改めて示しています。この種の事件で最も被害が大きかったのは、2005年に起きたCardSystems Solutions社のケースです。この事件では、約4,000万件のカード会員情報を暗号化せずに格納していたデータベースに対して不正アクセスが行われました。この他にも、数多くの著名な金融機関やサービス・プロバイダがセキュリティ侵害を受けています。2005年はこの種の事件が多発し、ワシントン・ポスト紙が「データ侵害の年」と名付けたほどでした。こうしたセキュリティ侵害事件が発生する状況は現在も変わっておらず、2006年5月には、米国退役軍人局が、氏名、住所、生年月日、社会保障番号を含む2,600万人分以上の個人情報が盗まれたことを明らかにしています。

データ・セキュリティ侵害に伴うコストは、直接的にも間接的にも、非常に甚大なものになる可能性があります。こうしたコストには、法律上の罰金やカード会社から課せられる金銭的ペナルティ、カードの再発行や交換に必要な費用、訴訟費用、各種の補償費用や修復費用などがあります。しかし、最大のコストは、企業の社会的信用が失墜したり、ビジネス機会が失われたりするおそれがあることです。

2005年6月30日に発効したPCI規格は、それまでMasterCardやVisaといったペイメント・カード会社各社がカード・システムのセキュリティを統制するために導入していた独自の規格を一本化したもので、世界のカード業界で採用されています。2006年9月にはバージョン1.1が発表され、PCI 1.0の条項の明確化と細かな改訂が行われました。PCI規格以前、Visaは、米国内ではCardholder Information Security Program (CISP)、米国外ではAccount Information Security (AIS) というプログラムを採用していました。またMasterCardは、Site Data Protection (SDP) というプログラムを自社のセキュリティ基準として運用していました。American Express、Discover Card、JCB (旧Japan Credit Bureau) も独自の規格を制定していましたが、のちに業界標準としてPCIを承認、採用して、MasterCardおよびVisaと手を結んでいます。

PCI規格は、この10年ほどの間に登場した多くの規制、例えばBasel II (新BIS規制)、Gramm-Leach-Bliley Act (GLBA: 米国金融制度改革法)、Health Insurance Portability and Accountability Act (HIPAA: 医療保険の相互運用性と説明責任に関する法律)、Sarbanes-Oxley Act of 2002 (サーベンス・オクスリー法: 米国企業改革法、略称SOX法)、各種の州法 (カリフォルニア州公告第1386号など) の中で、最も包括的なセキュリティ基準の1つであると言われています。PCI規格は、6つの概略的な分野と12の要件を定めており、その下に具体的な要件を規定しています。その分野と要件を表1に示します。

PCI規格で規定されている要件の概要

安全なネットワークの構築と維持

1. カード会員情報を保護するため、ファイアウォールを導入し、適切な設定を維持する。
2. システム・パスワードなどのセキュリティ・パラメータをデフォルト値のままにしない。

カード会員情報の保護

3. 保存されているカード会員情報を保護する。
4. カード会員情報を公衆網経由で送信する場合は暗号化を行う。

脆弱性管理プログラムの導入

5. アンチウイルス・ソフトウェア/プログラムを導入し、定期的に更新する。
6. 安全性の高いシステムおよびアプリケーションを開発し、保守する。

強固なアクセス制御手段の実装

7. カード会員情報へのアクセスを業務上必要な範囲に限定する。
8. コンピュータ・アクセスを行う各ユーザに一意のIDを割り当てる。
9. カード会員情報への物理的なアクセスを制限する。

ネットワークの監視と定期的な検査

10. ネットワーク・リソースおよびカード会員情報へのすべてのアクセスを追跡および監視する。
11. セキュリティ・システムおよびセキュリティ・プロセスを定期的に検査する。

情報セキュリティ・ポリシーの策定と運用

12. 情報セキュリティに関するポリシーを策定し、運用する。

表1

PCI規格の対象者

PCI規格は、当該ペイメント・カードに加盟し、カード会員情報を保管、処理、送信するすべての銀行、加盟店、サービス・プロバイダ（第三者の処理業者やデータ管理業者など）に適用されます。PCI規格の要件は、すべての「システム・コンポーネント」に適用されます。「システム・コンポーネント」とは、カード会員情報を扱う環境に含まれる（あるいはその環境に接続される）あらゆるネットワーク・コンポーネント、サーバ、アプリケーションのことを意味しています。「ネットワーク・コンポーネント」とは、ファイアウォール、ネットワーク・アプライアンス、ルータ、スイッチ、無線アクセス・ポイントと、その他のネットワーク・コンポーネントおよびセキュリティ・コンポーネントのことを指しています。「サーバ」には、認証サーバ、データベース・サーバ、DNS (Domain Name Service) サーバ、メール・サーバ、NTP (Network Time Protocol) サーバ、プロキシ・サーバ、Webサーバが含まれます（ただし、これらに限定されません）。「アプリケーション」には、既成のアプリケーションとカスタム・アプリケーション、内部アプリケーションと外部 (Web) アプリケーションのすべてが含まれます。したがって、小規模、中規模、大規模のすべての事業者が影響を受けることになります。また各要件は、電話、Web、郵便、店舗のすべての決済チャネルに適用されます。

加盟店銀行（加盟店の決済処理を行う銀行）では、自身についてだけでなく、契約している加盟店およびサービス・プロバイダについても、PCI規格への準拠を保証することが求められる場合があります。この場合、加盟店銀行は、電子商取引での年間取引件数が2万件を超えるすべての加盟店について、PCI規格に準拠していることを証明する必要があります。

PCI規格の4つの準拠レベル

PCI規格では、取引件数、決済チャネル、および企業間でのデータの取り扱いレベルに応じて、複数の段階を設定しています。加盟店は、以下の表に示すように4つのレベルに分類されます。各加盟店は、そのレベルに応じて、訪問調査、セキュリティ自己診断、ネットワーク・セキュリティ・スキャンなど、複数の検証作業を実施する必要があります。例えば、レベル1の加盟店は、認定監査機関が実施する年1回の訪問調査と四半期ごとのネットワーク・スキャンに合格する必要があり、レベル2の加盟店は、年1回の自己診断を実施し、四半期ごとのネットワーク・スキャンに合格する必要があります。

MasterCardとVisaは、最近になって加盟店のレベル定義を変更しています。以前は、「電子商取引での年間取引件数が15万件から600万件」と定義されていたレベル2が、「すべてのチャネルでの年間取引件数が100万件から600万件」に変更されました。この結果、以前はレベル4に分類されていた約1,000の加盟店がレベル2に、若干数がレベル2からレベル3に変更となっています。

加盟店のレベルの分類

レベル	基準	必要な検証作業	検証者
レベル1	チャネルを問わず、年間取引件数が600万件を超える加盟店 / チャネルを問わず、過去にセキュリティ侵害が発生したことのある加盟店	年1回の訪問調査	認定データ・セキュリティ企業 (Qualified Data Security Company: QDSC) または内部監査
		四半期ごとのネットワーク・スキャン	第三者の認定スキャン・ベンダー
レベル2	チャネルを問わず、年間取引件数が100万件～600万件的加盟店	年1回の自己診断	加盟店
		四半期ごとのネットワーク・スキャン	第三者の認定スキャン・ベンダー
レベル3	電子商取引での年間取引件数が2万件～100万件的加盟店	年1回の自己診断	加盟店
		四半期ごとのネットワーク・スキャン	第三者の認定スキャン・ベンダー
レベル4	電子商取引での年間取引件数が2万件未満の加盟店 / 年間取引件数が最大100万件的加盟店	年1回の自己診断と年1回のネットワーク・スキャンを推奨	

サービス・プロバイダのレベルの分類 (Visaサービス・プロバイダ)

レベル	基準	必要な検証作業	検証者
レベル1	すべてのVisaNet 処理業者(メンバー および非メンバー) / すべての決済 ゲートウェイ	年1回の訪問調査	認定データ・ セキュリティ企業 (Qualified Data Security Company:QDSC) または内部監査
		四半期ごとのネット ワーク・スキャン	第三者の認定 スキャン・ベンダー
レベル2	レベル1には該当 しないが、年間100万 件を超えるVisaアカ ウント / 取引を保管、 処理、または送信する サービス・プロバイダ	年1回の訪問調査	認定データ・ セキュリティ企業 (Qualified Data Security Company:QDSC) または内部監査
		四半期ごとのネット ワーク・スキャン	第三者の認定 スキャン・ベンダー
レベル3	レベル1には該当しな いが、年間100万件未 満のVisaアカウント / 取引を保管、処理、 または送信するサー ビス・プロバイダ	年1回の訪問調査	サービス・プロバイダ
		四半期ごとのネット ワーク・スキャン	第三者の認定 スキャン・ベンダー

ペイメント・カード決済の仕組み

PCI規格がもたらす課題と機会を深く理解するためには、ペイメント・カード決済の全体の流れを把握しておくことが重要です。ペイメント・カードの磁気ストライプには、カード会員の氏名、カード番号、有効期限、カードの有効性を検証するためのデータ、そしてカード発行者固有の情報が記録されています。カード会員が、電話、Web、郵便、店舗のいずれかのチャンネルを通じて加盟店から商品やサービスを購入すると、カードの情報は、電話オペレータや電子商取引システム、POS端末に渡されます。磁気ストライプに記録されている一部のデータ(検証用のデータ)は、加盟店からその加盟店銀行(または第三者の処理業者)に送信され、さらにカード会社を経由してカード発行銀行に送られて与信確認が行われます。取引データは、別のフロー(および後のフロー)で同じ関係事業者に送られます。そして最後に、カード会社の決済ネットワークを通じて支払いが行われます。

加盟店などがどの情報を送信および保管できるか(および誰に送信できるか)については、制限と指針が設けられていますが、これらの規定は正しく運用されているとは言えないのが現状です。例えば、取引が正当なものであることを証明する責任は加盟店にあります。そのため多くの加盟店は、このことを証明できるように、できる限り多くの情報を手元に置いておこうとします。このことが、カード会員情報の侵害リスクを高めてしまっています。

もしPCI規格が、電子決済システムに関わる一部の事業者にしか適用されなければ、データ・セキュリティに瑕疵が生じます。そのため加盟店には、自らが取り扱うカード会員情報にアクセスするすべての第三者についても、PCI規格を遵守させる責任が課せられています。また加盟店銀行も、加盟店の規格遵守に責任を負っています。

期限と罰則

加盟店は、2005年6月30日までにPCI規格への準拠を完了する必要がありました(サービス・プロバイダは2004年9月30日)。カテゴリがレベル2へと変更になった加盟店は、2007年9月30日までに準拠を完了する必要があります。PCI規格に準拠していない場合は、最高50万ドルの罰金とセキュリティ・インシデント1件につき最高10万ドルの罰金を科せられる場合があります。また最悪の場合には、ペイメント・カード会社との取引が一時停止、あるいは契約解除となることもあります。

しかし通常、企業にとって最も大きな損害は、社会的信用が失われることです。大規模なセキュリティ侵害が発生した企業では、顧客を失い、特定の販売チャネルでの信頼を失い、さらに株式を公開している場合には株価が下落するおそれがあります。

またセキュリティ侵害が発生した場合、不正利用されたカードを交換したり再発行したりするために、カード1枚につき最大50ドルのコストを強いられます。加えて、各種の補償費用や修復費用、さらに場合によっては訴訟費用も発生します。PCI規格では、セキュリティ・インシデントが発生した場合には、直ちに対策を施し、カード会員情報の漏洩を最小限に抑え、ペイメント・カード会社および加盟店銀行に連絡して詳細を報告することが求められています。

理解しておく必要があるのは、PCI規格への準拠は、「いったん完了すればそれで終わり」というものではないということです。PCI規格の第6要件では、安全性の高いシステムおよびアプリケーションを運用管理し、新しいセキュリティ・ベスト・プラクティスやセキュリティ・ソリューションが登場したら、それに合わせてシステムおよびアプリケーションを刷新していくことが求められています。

PCI規格の認定監査機関とスキャン・ベンダーの役割

レベル1の加盟店およびサービス・プロバイダに対して規定されている訪問調査は、認定データ・セキュリティ企業 (QDSC) が実施する必要があります。Master CardとVisaは、QDSC認定を希望するベンダー向けのプログラムや、スキャン・サービスを実施する企業を認可するプログラムを制定しています。またこの両社は、検査などのセキュリティ関連業務を実施する認定データ・セキュリティ専門家 (Qualified Data Security Practitioner: QDSP) をトレーニングする認定プログラムも提供しています。認定監査機関およびスキャン・ベンダーの一覧は、ペイメント・カード会社のWebサイトで提供されています。

QDSCやスキャン・ベンダーの多くは、ベスト・プラクティス・セキュリティ評価や、規格への対応状況をチェックするレビュー作業、システム導入およびトレーニング、システム・インテグレーションといったセキュリティ関連、ネットワーク関連の付加価値サービスも提供しています。

QDSCとしての認定を受けるための要件

QDSCとしての認定を受けるためには、ビジネス面での要件 (財務状況、信用履歴、保険によるカバー範囲)、技術面での要件 (セキュリティ評価の実施経験、セキュリティ業務への注力度)、そして管理面での要件をそれぞれ満たす必要があります。認定には、手数料とオンサイト・トレーニング料金が必要となります。

米国と欧州の違い

PCI規格は国際標準ですが、ペイメント・カードを巡る状況は、米国と欧州 (およびその他の諸地域) では大きく異なります。クレジットカードを中心とするペイメント・カードの利用は、米国外ではそれほど一般的ではなく、また決済システム全体 (ペイメント・カードに加盟している金融機関の数、決済インフラストラクチャ、第三者の処理業者の存在) を見ても、米国が最も成熟しています。例えば欧州では、各国の決済インフラストラクチャがパッチワーク的に接続されて全体のシステムが構成されています。そのため欧州中央銀行は、市場をよりオープンかつ整合性のあるものにするために、2010年の実現を目指して単一ユーロ支払地域 (Single Euro Payments Area: SEPA) の樹立に取り組んでいます。

一方、欧州が米国に先行している部分もあります。欧州のペイメント・カードでは、磁気ストライプ方式ではなく、「Chip and PIN」方式 (スマート・カード技術) が採用されています。このチップには、カードに関する情報が暗号化された状態で記録されており、カード会員は、カードでの支払い時に署名を行う代わりに4桁の暗証番号 (Personal Identification Number: PIN) を入力します。これにより、カードのデータを盗まれにくくしています。

Chip and PIN方式が採用されていること以外に、欧州の方が個人情報盗難の被害が少ない理由としては、次のことが挙げられます。社会保障番号が個人の識別情報として広く使用されている米国と異なり、欧州では、社会保障番号は社会保障のためにしか使用されません。英国を除く欧州のほとんどの国々では国民IDカードを導入しており、また多くの信用調査機関では独自の識別番号を使用しています。そのため欧州では、米国ほど簡単に個人の金融情報が流布することがないのです。また、ほとんどの西欧諸国では、企業が個人情報を共有したり売買したりすることが法律で制限されています。例えば、EUのプライバシー指令は、公開されている情報からデータを収集することを制限しています。

とは言え、欧州各国でこれらの情報を利用した詐欺が発生していないというわけではありません。英国小売協会によれば、2005年にクレジットカード詐欺が英国の小売業者に与えた損害は、推定22億ユーロ (41億ドル) にもなります。PCI規格の欧州における前身であるVisaのAccount Information Security (AIS) 規格は、欧州の次なる論理的追加防衛策と呼ばれていました。

PCI規格の課題

PCI規格が包括的で網羅的な内容になっているということに関しては、ほとんど異論は出ていません。例えばHIPAAなどと比較しても、要件は明確かつ簡潔に記述されています。また、明示的な分類はなされていませんが、技術面、管理面、そして物理面というデータ・セキュリティの重要な側面はすべてカバーされています。

PCI規格の特徴であり課題であることの1つは、規格に準拠しているかどうか「オール・オア・ナッシング」であるということです。つまり、加盟店やサービス・プロバイダが全要件の99パーセントを満たしていたとしても、規格自体には準拠できていないことになってしまうのです。Gartner Groupは、PCI規格に準拠できている企業が予想よりも少ないのは、このことが主な理由だと指摘しています。この点については、最新版のPCI 1.1から改善の取り組みが始まっています。

加盟店が直面しているもう1つの課題は、低コストかつ統一された方法で規格に準拠することです。複数のポイント・ソリューションを購入して統合するという方法は、時間と労力が必要とされるうえに運用管理が難しく、またセキュリティ状態の全体像を把握することも困難になりがちです。

また、PCI規格の対象となる企業はパフォーマンスに関しても懸念を示しており、セキュリティ・コンポーネントやセキュリティ・ポリシーを追加することによって、顧客が直接的に関与する重要なプロセスの処理速度が低下するといった事態を危惧しています。

現在では、ほとんどの組織が、複数の規制や規格に対応することを迫られています。こうした組織では、他の規制や規格にはない要件と他と重複する要件をいかにして確実かつ効率的に管理するかが重要となります。これは、監査、レポート、インシデント調査といった作業にも言えることです。

またPCI規格では、加盟店の代理としてカード会員情報を保管、処理、送信するサービス・プロバイダが規格に準拠できていなければ、その加盟店も規格に準拠していることになりません。つまり、ベンダーやサービス・プロバイダのシステムおよび管理状況についても詳しく調査しなければならないという新たな重荷が、多くの組織に課せられているのです。

PCI規格に準拠するための検討項目

このような課題はあるものの、カード会員情報を取り扱う企業は、強力かつ生産的な手段を用いることによって、PCI規格への準拠を実現すると同時に、その他の複数の規制に対応し、インフラストラクチャを合理化するなどビジネス面でも大きなメリットを享受することが可能になります。

PCI規格の対象となる企業は、必要な対策を検討し、講じるにあたって、次の点を考慮する必要があります。

1. 複数の要件を満たすことのできるソリューションを提供する、信頼あるベンダーを選ぶ。ベンダーによっては、ポイント・ソリューション（アンチウイルス、アクセス認証 / 認可、侵入防御などの特定機能のみを提供するソリューション）しか提供していない場合もあります。また、フォレンジック・ツールやレポート・ツールなど、インシデント発生後の監査証跡の確保に役立つツールのみを提供し、インシデントを検出したり防止したりするツールを提供していないベンダーもあります。これらの各機能が統合されたソリューションであれば、運用管理などの面で効率化を図ることができます。
2. 可能な場合には、全体論的な観点から規格や規制への準拠を考える。他の規制への準拠にも役立つコア・セキュリティ機能を備えたソリューションを選択するようにします。コア・セキュリティ機能の例としては、アクセスおよび認証、プライベート・ネットワーク / ファイアウォール、セキュリティ・インシデントの監視 / 複数のデバイスにまたがるインシデントの検出、悪意あるソフトウェアのブロック、暗号化、集中管理（ソフトウェアのアップデートやレポート）などがあります。
3. ビジネス面で大きなメリットをもたらす、他社との差別化を図ることが可能なソリューションを評価、検討する。例えば加盟店の場合には、業務効率の向上、サービスや取引チャネルの新設、ビジネスの継続性維持、カード会員の信頼性維持、全体的な顧客満足の向上といったことを実現できるかどうかを考慮します。
4. 企業の成長を可能にする、強固なコンプライアンス・ソリューション基盤を構築する。すでに述べたとおり、PCI規格は「いったん完了すればそれで終わり」という種類の要件ではありません。企業組織の変化（営業所の新設、新しい販売チャネルの導入など）に対応し、最新のセキュリティ上の脅威に対処して、新しい技術やセキュリティ・ベスト・プラクティスを導入していくためには、ソリューションを常に監視し、手を加えていくことが必要です。

PCIバージョン1.1

2006年9月、PCI規格の改訂版が発布されました。この改訂版では、次のような変更が行われています。

- カード会員情報の特定のデータ要素と、その保管および保護に関する要件を明確化した新しい条項の追加
- その要件が適用される期間の明確化
- ホスティング・プロバイダに適用される要件の明確化
- PCI 1.0で定められている、カード会員情報を容易には読み取れないようにするための要件を完全には遵守できない企業などを対象とする、その補完手段に関する条項の追加
- アプリケーション・ファイアウォールの使用に関する新しい要件の追加（2008年6月30日までは随意、それ以降は義務化）
- PCI 1.0で曖昧だった表現全般の明確化

この改訂版はPCI 1.0に置き換わるものですが、2006年12月31日まではPCI 1.0をPCI準拠の基準として使用できることになっています。ただし、それ以降はPCI 1.1の使用が義務化されます。

PCI規格の各要件に対応するチェック・ポイントのソリューション

以下の表に示すように、チェック・ポイントのソリューションは、PCI 1.1で規定されているセキュリティ要件の大部分(特に技術的な要件)に対応しています。チェック・ポイントのコア製品ではカバーできないいくつかの領域(プロセスに関する要件など)については、それぞれの分野をリードするさまざまなチェック・ポイント・パートナーが必要な機能やサービスを提供しています。チェック・ポイントの製品をPCI規格準拠の基盤として導入すると、他のセキュリティ規格で規定されている数多くの要件も同時に満たすことができます。チェック・ポイントとOPSECパートナーが提供する包括的な統合セキュリティ・ソリューションは、企業の成長を支える強力な基盤の構築を可能にします。PCI DSSバージョン1.1の全文については、<https://www.pcisecuritystandards.org>をご覧ください。

要件	チェック・ポイントのソリューション
1. カード会員情報を保護するため、ファイアウォールを導入し、適切な設定を維持する	
<p>1.1 ファイアウォールの設定基準を確立する。</p>	<p>業界最高レベルの実績を誇るステートフル・ファイアウォール・ソリューションVPN-1®(先進のファイアウォール製品FireWall-1®を統合)は、セキュリティ対策の最前線であるファイアウォールのまさにスタンダードです。VPN-1は、この要件を含め、ファイアウォールに関するPCI規格のすべての要件をサポートします。VPN-1は、第1.1項の下位要件に定められている、ネットワーク・コンポーネントのきめ細かな論理的管理、内部ネットワーク・ゾーンのセグメント化によるカード会員情報 / ネットワークの各部の保護、ポートの割り当ておよび文書化、ファイアウォール設定のポリシー策定、監査およびレポート、ネットワーク接続の図示などに対応する機能を備えています。</p> <p>チェック・ポイントのセキュリティ管理アーキテクチャSMART™により、管理者は、ネットワーク・トポロジを集中的に管理、承認、および表示し、すべての外部ネットワーク接続やファイアウォール設定の変更を検証することができます。ファイアウォールのセキュリティ・ポリシー、プロトコル、およびルール・セットを一覧表示したり、ファイアウォールのポリシーを集中管理して複数のVPN-1ゲートウェイに一括適用したりすることも可能です。</p> <p>また、チェック・ポイント認定の取り扱い販売店、システム・インテグレータ(SI)、およびビジネス・パートナーは、第1.1項で規定されているプロセスおよび文書化に関する要件に対処するためのコンサルティング・サービスを提供しています。</p>
<p>1.2 カード会員情報を扱う環境に必要なプロトコルを除き、「信頼できない」ネットワークおよびホストからのトラフィックをすべて拒否するようにファイアウォールを設定する。</p>	<p>VPN-1では、「明示的に許可されていないものは禁止する」というアプローチを採用しています。したがって、ファイアウォールのセキュリティ・ポリシーで定義されているトラフィックのみがVPN-1のファイアウォールを通過することを許可します。このため、「信頼できない」ネットワークおよびホストからのトラフィックのみを拒否しつつ、Webプロトコル、システム管理プロトコル、その他環境に必要なプロトコルのトラフィックのみを許可するセキュリティ・ポリシーは簡単に設定することが可能です。チェック・ポイントの統一セキュリティ・アーキテクチャでは、セキュリティ・ポリシーや設定の更新をすべてのゲートウェイに簡単に配布できるため、一貫性のあるポリシーの実施と業務効率の向上が実現されます。</p>

要件	チェック・ポイントのソリューション
<p>1.3 公開サーバとカード会員情報を格納するシステム・コンポーネントの間の接続（無線ネットワークからの接続を含む）を制限するようにファイアウォールを設定する。</p>	<p>VPN-1では、ネットワークを複数のゾーンにセグメント化し、ネットワーク・セグメント間にセキュリティ・ポリシーを適用することで、機密性の高いネットワーク・コンポーネントやネットワーク・セグメント（カード会員データベース、ファイル・サーバ、プリント・サーバなど）を公開サーバから保護することができます。この機能により、第1.3項の大半の項目を費やして規定されている、「信頼できる」ネットワーク、DMZ、無線ネットワーク、および「信頼できない」ネットワークのセグメント化が可能になります。</p> <p>ステートフル・インスペクション技術のパイオニアであるチェック・ポイントの製品は、第1.3.3項の下位要件「ネットワークの包括的な保護を実現するために、すべての通信のステートおよびコンテキストを追跡可能であること」を当然のこととして満たしています。VPN-1は、内向き / 外向きフィルタと、着信 / 発信トラフィックを制限する機能を備えており、カード会員情報を扱う環境に必要なトラフィックのみ通過を許可することができます。また、IPアドレス・スプーフィングの検出にも対応しているため、内部アドレスを持つトラフィックがインターネットからDMZに侵入するのを防止することもできます（第1.3.2項）。</p> <p>チェック・ポイントのエンドポイント・セキュリティ・ソリューション・スイートCheck Point Integrity™は、業界で最も実績のあるパーソナル・ファイアウォールZoneAlarm®の防御技術をベースとしています。Integrityを使用することで、インターネットへの接続機能を持つモバイル・デバイスや従業員の私用PCからのアクセスを制限できます（第1.3.9項）。</p>
<p>1.4 外部ネットワークとカード会員情報（データベース、ログ、トレース・ファイルなど）を格納するシステム・コンポーネントの間の直接的な公開アクセスを禁止する。</p>	<p>VPN-1では、一部のトラフィックまたはすべてのトラフィックを遮断するようにDMZを定義できます。これにより、着信 / 発信のインターネット・トラフィックの直接ルーティングを禁止したり、DMZからの発信トラフィックを禁止したりできます（第1.4項）。</p>
<p>1.5 内部アドレスがインターネット上で変換されたりインターネット側に露呈したりしないように、IPマスカレードを実装する。ポート・アドレス変換（PAT）やネットワーク・アドレス変換（NAT）などのRFC 1918のアドレス空間を実装した技術を使用する。</p>	<p>VPN-1には、内部アドレスがインターネット側に露呈することを防止する幅広いIPマスカレード機能が用意されています。VPN-1ではNAT技術を使用しますが、SMART管理アーキテクチャにより、組織全体にわたってNATポリシーを定義したり、ポリシーをまとめて表示してこれらが適切に適用されているかどうかを確認したりといったことが容易に行えるようになっています。</p>

要件	チェック・ポイントのソリューション
2. システム・パスワードなどのセキュリティ・パラメータをデフォルト値のままにしない	
<p>2.1 システムをネットワーク上に配置する前に、必ずデフォルト設定を変更する(パスワードやSNMPコミュニティ文字列を変更する、不要なアカウントを削除するなど)。</p>	<p>チェック・ポイントのソリューションには、完全インストールの前にデフォルト設定を変更するようユーザに促す仕組みが備わっています。例えばVPN-1では、初期インストールの際にデフォルトのパスワードを変更することが必須となっています。さらに、推測可能な情報を用いてアクセスを試みるハッカー対策として、脆弱なパスワードは使用できないようになっています。</p> <p>VPN-1 UTM Edge™ Wireless (W) は、Wi-Fi Protected Access (WPA) 技術を用いて、第2.1項の下位要件で規定されている無線トラフィックの暗号化と認証を行います。</p> <p>VPN-1ソリューションでは、集中管理環境でパスワードや暗号鍵などの設定を規定し、各地の営業所などにあるリモート・デバイスに配信することができます。</p> <p>チェック・ポイントのVAR、SI、およびビジネス・パートナーは、チェック・ポイントのソリューションを用いて、第2.1項で規定されているこれらのセキュリティ・チェックをネットワークの各所で正しく実施するためのコンサルティング・サービスを提供しています。</p>
<p>2.2 すべてのシステム・コンポーネントについて設定基準を策定する。規準の策定にあたっては、既知のすべてのセキュリティ脆弱性に対処し、SysAdmin Audit Network Security Network (SANS)、National Institute of Standards Technology (NIST)、Center for Internet Security (CIS) など定められている業界のシステム強化規準と矛盾がないようにする。</p>	<p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、第2.2項で規定されているコンポーネントの設定に関する要件に対処するためのコンサルティング・サービスを提供しています。ただし、チェック・ポイントのソリューションでも、特定のサービス(DNSやWebなど)だけが適切なサーバにアクセスできるようにし、不要なサービスはアクセスできないようにすることで、この条項の目的を補完することができます。</p> <p>また、チェック・ポイントのSmartDefense™サービス、Application Intelligence™技術、Web Intelligence™技術では、アプリケーション・レベルのトラフィックを検査することで、対象サーバへのアクセスを許可されているプロトコルやサービスに含まれる悪意あるコードをブロックすることができます。SmartDefenseサービスは、今日の、絶えず進化を遂げる脅威の常に一歩先を行くことを可能にするため、各種のアップデートや、防御機能およびセキュリティ・ポリシーの設定アドバイザリをリアルタイムかつ継続的に提供します。SmartDefenseサービスでは、セキュリティ設定および防御機能は単一の統合インタフェースから一括して更新することができるため、セキュリティ・システムは常に最新の状態に維持され、新たに出現した脅威にも対処できるようになります。</p> <p>チェック・ポイント製品は、製品と管理ソフトウェア間で行われる非コンソール管理アクセスの通信を、チェック・ポイントのSecure Internal Communication (SIC)、SSH、およびSSLを使用して暗号化することにより、通信の安全性と機密性を維持します。また、VPN-1やConnectraなどのセキュリティ・ゲートウェイ・ソリューションでは、非コンソール管理アクセスのためのVPN暗号化機能を持たない外部システムに、この機能を提供することができます。</p>

要件	チェック・ポイントのソリューション
<p>2.3 非コンソール管理アクセスはすべて暗号化する。Webベースの管理などの非コンソール管理アクセスには、SSH、VPN、SSL / TLS (Transport Layer Security) などの技術を使用する。</p>	<p>チェック・ポイント製品は、製品と管理ソフトウェア間で行われる非コンソール管理アクセスの通信を、チェック・ポイントのSecure Internal Communication (SIC)、SSH、およびSSLを使用して暗号化することにより、通信の安全性と機密性を維持します。また、VPN-1やConnectraなどのセキュリティ・ゲートウェイ・ソリューションでは、非コンソール管理アクセスのためのVPN暗号化機能を持たない外部システムに、この機能を提供することができます。</p>
<p>2.4 ホスティング・プロバイダは、各事業者の環境およびデータを保護しなければならない。ホスティング・プロバイダは、「付録A:ホスティング・プロバイダに適用されるPCI DSSの要件」に示す特定の要件を満たす必要がある。</p>	<p>VPN-1 Power VSX™は、バーチャル・ネットワーク環境を構築しているマネージド・サービス・プロバイダおよび大規模企業において、単一のハードウェア・プラットフォーム上に最大250のバーチャル・セキュリティ・システム(ファイアウォール、VPN、および侵入防御の各機能を含む)を構築することを可能にするバーチャル・セキュリティ・ゲートウェイです。これによりサービス・プロバイダでは、付録A.1で規定されているように、各事業者のカード会員情報を相互に隔離し、事業者によるカード会員情報へのアクセスをその事業者が管理する情報だけに制限することが可能になります。また、各事業者のログを、他の事業者のログとは別個に格納および管理することもできます。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、付録A.1の要件に従ってネットワークを正しく構成し、情報の保存に関する付録A.1.4の要件に従ってプロセスを定義するためのコンサルティング・サービスを提供しています。</p>
<p>3. 保存されているカード会員情報を保護する</p>	
<p>第3項は、チェック・ポイントのソリューションが関与しない管理要件(ポリシー設定)および保存要件について規定しています。第3項で規定されている暗号化戦略は、主にカード会員情報の保存について述べたものであり、暗号化されたVPN通信については次の第4項で規定されています。</p> <p>PCI 1.1では、カード会員情報を読み取れないようにするための第3.4項の要件を満たすことのできない企業のために、付録Bが追加されています。付録Bでは、正当な技術的理由がある場合に、補完手段を用いてこの要件に準拠する方法が定められています。チェック・ポイントのVPN-1とInterSpect™は、ここで規定されているネットワークのセグメント化、アクセス制限、データベース・アクセス、およびアプリケーション / データベースへの攻撃に対処するためのセキュリティ制御に関する機能を提供しています。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、組織が保存しているカード会員情報の保護に関するこの条項の要件に対処するためのコンサルティング・サービスを提供しています。</p>	

要件	チェック・ポイントのソリューション
4. カード会員情報を公衆網経由で送信する場合は暗号化を行う	
<p>4.1 オープンな公衆網経由で機密性の高いカード会員情報を送信する場合は、SSL (Secure Sockets Layer) / TLS (Transport Layer Security) やIPSec (Internet Protocol Security) などの強力な暗号化技術とセキュリティ・プロトコルを使用してこれらを保護する (下位要件として無線ネットワークの暗号化を含む)。</p>	<p>チェック・ポイントのリモート・アクセス・ソリューションであるVPN-1とConnectraは、公衆網経由でデータを送信する際、標準ベースの暗号化プロトコルを使用して強力な暗号化を行います。VPN-1は、SSLとIPSecによる暗号化通信をサポートしています。Connectraは、SSLとTLSによる暗号化通信をサポートしています。またどちらの製品も、カード会員情報を含む安全な通信の完全性を保証するためのMD5とSHA-1をサポートしています。</p> <p>ソリューションの一機能としてWi-Fiアクセスを提供するVPN-1 UTM Edge Wirelessは、IPSec-over-WLANによる暗号化を採用し、WEPキーを定期的にローテーションします。VPN-1 UTM Edge Wirelessは、WEP、WPA、WPA-PSKの安全性を高めるために、チェック・ポイントのファイアウォール、侵入防御、およびアンチウイルスの各技術を用いて検査を行います。IPSec over WLANを使用するユーザには、WEPを使用するユーザよりも上位のアクセス権を付与することもできます。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータは、および販売代理店は、チェック・ポイントのソリューションを用いて、第4.1項で規定されている暗号化通信に関する要件に対処するためのコンサルティング・サービスを提供しています。</p>
<p>4.2 暗号化していない電子メールでカード番号 (Primary Account Number : PAN) を送信しない。</p>	<p>VPN-1やConnectraなどのチェック・ポイントのリモート・アクセス・ソリューションでは、この条項で規定されているように、PANが記述されている可能性のある電子メールの通信は必ず暗号化するように設定することができます。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータは、および販売代理店は、チェック・ポイントのソリューションを用いて、この条項で規定されている電子メール・システムによる暗号化通信に関する要件に対処するためのコンサルティング・サービスを提供しています。</p>

要件	チェック・ポイントのソリューション
5. アンチウイルス・ソフトウェア / プログラムを導入し、定期的に更新する	
<p>5.1 ウイルスの影響を受けやすいすべてのシステム(PCやサーバなど)にアンチウイルス・ソフトウェアを導入する。</p>	<p>VPN-1ファミリ (UTM-1、VPN-1 UTM、VPN-1 UTM Edge、VPN-1 UTM Power) には、ゲートウェイ・ベースのアンチウイルス機能が統合されています。ゲートウェイ・ベースのアンチウイルス機能は、個々のPCやサーバに導入されているアンチウイルス・ソリューションを補完し、より広範な脅威に対処できるようにします。</p> <p>エンドポイント・セキュリティ製品のIntegrityは、従来のシグネチャ・ベースのウイルス対策を回避して短時間のうちに広まるウイルスやワーム (Blaster、MyDoom、Sasserなど) をブロックするために必要な事前防御の仕組みを提供します。Integrityは、デスクトップ・ファイアウォール機能とアプリケーション制御機能を組み合わせることにより、マルウェアのブロック、スパイウェアの除去、およびバッファ・オーバーフロー攻撃への対処を自動的に行うと共に、ユーザがインスタント・メッセージ (IM) を安全に使用できるようにします。また、アンチウイルス・ソリューションの使用を強制することもできます。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、チェック・ポイントのソリューションを用いてこの条項の要件に対処したり、導入済みのアンチウイルス・ソリューションとチェック・ポイントのソリューションを連携させたりするためのコンサルティング・サービスを提供しています。</p>
<p>5.2 すべてのアンチウイルス・メカニズムについて、最新の状態であり、正常に稼働しており、監査ログを生成可能であることを保証する。</p>	<p>Integrityは、シグネチャの更新とパッチの適用を自動的に行います。また、アンチウイルス・ソリューションの使用を強制することもできます。Integrityを使用することにより、ネットワーク中のすべてのエンドポイントが最新のアンチウイルス・メカニズムで保護されていることを保証できるようになります。Integrityは、ネットワークへの接続をPCに許可する前に、そのPCが組織のネットワーク・アクセス・ポリシーを遵守しているかどうかをチェックします。PCのアンチウイルス機能が最新の状態でない場合は接続を拒否し、それらのシグネチャとアンチウイルス・エンジンを自動的に更新します。Integrityは、自社の管理下にあるPCだけでなく、ゲストPCについてもネットワークへの接続を許可する前にセキュリティをチェックできるほか、監査およびフォレンジック分析に役立つ詳細なログ・データとフィルタリング可能なレポートも提供します。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、チェック・ポイントのソリューションを用いてこの条項の要件に対処したり、導入済みのアンチウイルス・ソリューションとチェック・ポイントのソリューションを連携させたりするためのコンサルティング・サービスを提供しています。</p>

要件	チェック・ポイントのソリューション
<p>6. 安全性の高いシステムおよびアプリケーションを開発し、保守する</p>	
<p>6.1 すべてのシステム・コンポーネントおよびソフトウェアに、ベンダーが提供する最新のセキュリティ・パッチを適用する。該当するセキュリティ・パッチはリリースから1か月以内に適用する。</p>	<p>Integrityでは、最新のアンチウイルス・ソリューションの使用を強制することのほか、組織のエンドポイントにネットワークへのアクセスを許可する前に、ポリシーで必須とされているWindowsのサービス・パックやパッチ、アプリケーション・パッチが適用されているかどうかをチェックすることができます。アンチウイルス機能と同様、適用されていないパッチをこれらのエンドポイントに自動的に送信し、バックグラウンドでインストールさせることができます。またIntegrityは、監査およびフォレンジック分析に役立つ、パッチ規則違反やその修復に関する詳細なログ・データとフィルタリング可能なレポートも提供します。</p> <p>SMART管理システムの一機能であるSmartUpdate™は、最新のソフトウェア・パッケージを一覧表示およびダウンロードする機能を提供し、チェック・ポイントのセキュリティ・ソリューションへの配信およびそのスケジュール設定を行えるようにします。これにより、すべてのチェック・ポイント・ソリューションが常に最新の状態に維持されます。</p> <p>またSmartDefenseサービスを使用すると、ソフトウェア、セキュリティ設定、および防御機能を単一の統合インタフェースから一括して更新することが可能になるため、セキュリティ・システムは常に最新の状態に維持され、新たに出現した脅威にも対処できるようになります。SmartDefenseサービスを使用することで、どのアップデートがダウンロード済みであるか、どのゲートウェイにそのアップデートが適用されているかも把握可能となります。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、第6.1項で規定されているベスト・プラクティスおよび文書化に関する要件に対処するためのコンサルティング・サービスを提供しています。</p>
<p>6.2 新たに発見されたセキュリティ脆弱性に関する情報を入手するためのプロセスを確立する（インターネットで無償提供されているアラート・サービスを購読するなど）。新しい脆弱性問題に対処するため、セキュリティ規準を改訂する。</p>	<p>SmartDefenseサービスは、チェック・ポイントが提供するセキュリティ・インフラストラクチャの事前防御的セキュリティを常に最新の状態に維持します。SmartDefenseサービスは、今日の、絶えず進化を遂げる脅威の常に一步先を行くことを可能にするため、各種のアップデートや、防御機能およびセキュリティ・ポリシーの設定アドバイザリをリアルタイムかつ継続的に提供します。また、新たに発見された脆弱性とそれに対する設定ポリシーをアラートとしてユーザに通知し、ネットワーク（さらにはカード会員情報）に対する潜在的なリスクに関する情報も提供します。アドバイザリでは、セキュリティ上の脅威に対処するためのベスト・プラクティスなどが提供されます。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、第6.2項で規定されているベスト・プラクティスおよび文書化に関する要件に対処するためのコンサルティング・サービスを提供しています。</p>

要件	チェック・ポイントのソリューション
<p>6.3～6.5 これらの条項は、安全なソフトウェアの開発およびテストに関する要件であり、チェック・ポイントのソリューションに直接関係するものではありません。</p> <p>ただし、Webベースのソフトウェア / アプリケーションの導入とコーディングに関する第6.5項については、その目的の達成を支援する追加レイヤとして、チェック・ポイントのソリューションを利用できます。VPN-1に統合可能なオプション・ソリューションWeb Intelligenceは、入力チェック、アクセス制御、スクリプティング/インジェクション攻撃のブロックなど、この条項の低位要件となっている機能を提供します。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、第6項で規定されているプロセス、ベスト・プラクティス、文書化に関する要件を満たす安全なシステムおよびアプリケーションの開発と保守を支援するコンサルティング・サービスを提供しています。</p>	
<p>6.6 次のいずれかの手法を用いて、既知の攻撃からすべてのWebアプリケーションを保護する。</p> <ul style="list-style-type: none"> ● アプリケーション・セキュリティを専門とする組織に、すべてのカスタム・アプリケーションのコードについて、一般的な脆弱性が含まれていないかどうかのチェックを依頼する。 ● アプリケーション・ファイアウォールをWebアプリケーションの手前に設置する。 <p>注意：この手法は、2008年6月30日まではベスト・プラクティスとして扱われますが、それ以降は必須の要件となります。</p>	<p>チェック・ポイントのWeb Intelligenceは、Web環境全体に対する包括な防御機能を提供するWebアプリケーション・ファイアウォール技術です。Web Intelligenceは、UTM-1、VPN-1 UTM、VPN-1 Power、VPN-1 UTM Edge、およびConnectraでサポートされており、その背後にあるネットワーク、オペレーティング・システム、Webサーバ、およびバックエンド・システムのためのマルチレイヤの防御機能を提供します。アプリケーションの手前に置かれたチェック・ポイントのゲートウェイにWeb Intelligenceを導入することで、この条項で規定されているアプリケーション・ファイアウォールの要件を満たすことができます。</p>

要件	チェック・ポイントのソリューション
<p>7. カード会員情報へのアクセスを業務上必要な範囲に限定する</p>	
<p>7.1 コンピューティング・リソースおよびカード会員情報へのアクセスを業務上必要なユーザだけに限定する。</p>	<p>アクセス制御は、チェック・ポイントのすべてのセキュリティ・ソリューションにとって不可欠な要素です。チェック・ポイントの境界、内部、Web、およびエンドポイント向けのソリューションでは、きめ細かなアクセス・ルールと権限付与ルールを作成することができます。VPN-1とInterSpectは、境界と内部ネットワーク上でアクセス・ポリシーを実施します。ConnectraとVPN-1は、境界の外にいるユーザにリモート・アクセスを許可する際にアクセス・ポリシーを実施します。Integrityは、デスクトップ・ファイアウォール・ルールとネットワーク・ゾーンを使用して、ネットワーク・リソースおよびネットワーク・セグメントへのPCアクセスを制限します。これらのアクセス・ポリシーでは、個人、グループ、または部門に対してどのリソースへのアクセスを許可するかを定義します。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、チェック・ポイントのソリューションを用いて、第7.1項に規定されているカード会員情報のアクセス制限に関する要件に対処するためのコンサルティング・サービスを提供しています。</p>
<p>7.2 複数のユーザが使用するシステムについて、ユーザの業務上必要な範囲に基づいてアクセスを制限し、明示的に許可しない限り「すべて拒否」に設定されるメカニズムを確立する。</p>	<p>チェック・ポイントの境界、内部、およびWeb向けの各ソリューションは、強力なアクセス制御の仕組みを備えています。アクセス権限は、個人、グループ、または部門の業務上必要な範囲に基づいて設定できるため、システム・リソース(カード会員情報など)へのアクセスは、そのリソースにアクセスする必要がある個人だけに制限することができます。またチェック・ポイントのソリューションには、管理者が明示的に許可しない限りデフォルトのアクセスを「すべて拒否」に設定する機能も用意されています。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、この要件に基づき、業務上必要な範囲と、チェック・ポイントのソリューションが実施するユーザ・アクセス・ポリシーを定義するためのコンサルティング・サービスを提供しています。</p>

要件	チェック・ポイントのソリューション
<p>8. コンピュータ・アクセスを行う各ユーザに一意のIDを割り当てる</p>	
<p>8.1 システム・コンポーネントまたはカード会員情報へのアクセスを許可する前に、すべてのユーザを一意のユーザ名で識別する。</p>	<p>認証は、VPN-1を含むVPNソリューションにおいてだけでなく、チェック・ポイントのすべてのソリューションにとって不可欠な要素です。VPN-1は、認証用に複数のデータベース(内部データベース、Microsoft Active Directory、OPSEC認定LDAP / RADIUSデータベースなど)をサポートしています。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、各ユーザに一意のIDを割り当てるIDプログラムをチェック・ポイントのソリューションと連携させるためのコンサルティング・サービスを提供しています。</p>
<p>8.2 ユーザを認証するにあたっては、一意のIDに加えて、次の要素を1つ以上使用する。</p> <ul style="list-style-type: none"> ● パスワード ● トークン・デバイス (SecurID、証明書、公開鍵など) ● バイオメトリクス 	<p>チェック・ポイントの各製品は、さまざまなユーザ認証メカニズムをサポートしています。VPN-1とConnectraは、保護されたカード会員情報へのアクセスに利用できる認証メカニズムとして、パスワード、トークン、デジタル証明書、およびワンタイム・パスワードをサポートしています。これらの認証メカニズムは、内部機能またはOPSECパートナーによる外部機能として提供されます。また一部のチェック・ポイント製品には、ユーザおよび事業者の認証に利用できる内部認証局(X.509デジタル証明書)も用意されています。これを利用すると、認証局を別途用意することなく事業者間で強力な認証を行うことが可能になり、シンプルな構成で第8.2項の要件を満たすことができます。さらに、VPNでの共有秘密鍵や、ユーザ名 / パスワード(ドメイン・パスワード)を使用する内部ユーザ・データベースもサポートされています。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、組織のニーズに最適で、チェック・ポイントのソリューションと連携でき、なおかつ第8.2項の要件を満たす認証メカニズムを選択および導入するためのコンサルティング・サービスを提供しています。</p>

要件	チェック・ポイントのソリューション
<p>8.3 従業員、管理者、および第三者によるネットワークへのリモート・アクセスには、2ファクタ認証を使用する。RADIUS (Remote Authentication Dial-In User Service) とトークン、TACACS(Terminal Access Controller Access Control System) とトークン、VPN (SSL / TLS またはIPSecベース)と個人証明書などの技術を使用する。</p>	<p>チェック・ポイントの多くのソリューションは、2ファクタ認証をサポートしています。VPN-1は、RADIUS、TACACS、トークン・カードなどのさまざまな認証オプションを提供しています。またVPN-1はOpenPKIをサポートしているため、Baltimore Technologies、Entrust、VeriSignといったベンダーが提供する主要PKIソリューションとの互換性が保証され、極めて大規模なIPSec VPN環境も管理することができます。チェック・ポイント独自のハイブリッド・モード認証により、SecurIDトークンなどの既存の認証スキームを活用しながらIPSec VPNを導入することが可能になります。</p> <p>製品の導入と同時に強力な認証を使用したいという場合には、チェック・ポイントのワン・クリック証明書を利用できます。VPN-1 Power、VPN-1 UTM、UTM-1およびVPN-1 UTM Powerには内部認証局が用意されており、VPN-1ゲートウェイおよびVPN-1 SecureClientユーザに対してX.509デジタル証明書を発行することができます。ワン・クリック証明書により、複雑で高コストなPKIシステムを構築することなく、業界標準の2ファクタ認証を導入することが可能になります。</p> <p>Connectraは、(LDAPおよびRADIUSの) ユーザ名 / パスワードの組み合わせと、PKI証明書またはサードパーティOPSECの認証トークンを使用する2ファクタ認証をサポートしています。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、各組織のニーズに最適で、チェック・ポイントのソリューションを補完し、なおかつこの要件を満たす認証システムおよび認証戦略を定義するためのコンサルティング・サービスを提供しています。</p>
<p>8.4 パスワードを送信する際、およびシステム・コンポーネントに保存する際は、必ず暗号化する。</p>	<p>パスワードは、送信の際はチェック・ポイントのSecure Internal Communication (SIC)を使用して完全に暗号化され、システム内部への保存時も暗号化されます。</p>
<p>8.5 すべてのシステム・コンポーネント上の非消費者ユーザおよび管理者について、適切なユーザ認証とパスワード管理を行う。</p>	<p>チェック・ポイントのアクセス・ソリューションは、すべてのシステム・コンポーネント上のすべてのユーザ (ゲスト・ユーザ、非消費者ユーザ、および管理者) に対する適切な認証とパスワード管理をサポートしています。チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、チェック・ポイントのソリューションが実施する、第8.5項のプロセス関連部分を定義するためのコンサルティング・サービスを提供しています。</p>
<p>9. カード会員情報への物理的なアクセスを制限する</p>	
<p>チェック・ポイントでは、物理的なアクセスを制限するセキュリティ・ソリューションは提供していません。</p> <p>チェック・ポイントのVAR、SI、およびビジネス・パートナーは、第9項で規定されているプロセス、ベスト・プラクティス、およびシステムを実装するためのコンサルティング・サービスを提供しています。</p>	

要件	チェック・ポイントのソリューション
10. ネットワーク・リソースおよびカード会員情報へのすべてのアクセスを追跡および監視する	
<p>10.1 システム・コンポーネントへのすべてのアクセス(特に、rootなどの管理者権限で行われるアクセス)と個々のユーザを関連付けるためのプロセスを確立する。</p>	<p>チェック・ポイントの管理ツールでは、グループ(ユーザとエンドポイント)のリソースへのマッピングおよび割り当てなどを行うためのポリシーを作成することができます。すべてのチェック・ポイント製品では、複数のゲートウェイにまたがるユーザ・アクセスや、管理者がシステムに対して行った変更をログに記録し、レポートすることができます。この情報は、SmartViewTracker™、またはEventia™ Reporterのレポートで確認できます。</p>
<p>10.2 次のイベントを再現可能な監査証跡を自動的に記録するための仕組みを実装する。</p> <ul style="list-style-type: none"> ● 個々のユーザによるカード会員情報へのアクセス ● root権限または管理者権限を持つユーザによるすべてのアクティビティ ● 監査証跡へのすべてのアクセス ● 無効な論理的アクセスの試み ● 識別/認証メカニズムの使用 ● 監査ログの初期化 ● システム・レベル・オブジェクトの作成および削除 	<p>チェック・ポイントのSmartCenterとEventia™ Suite (Eventia ReporterとEventia™ Analyzerを含む)は、システム・イベントおよびアクティビティのロギング、アップデート、監視、レポートリングを一元化することにより、セキュリティ・アクティビティおよびネットワーク・アクティビティの全体的な傾向を把握できるようにします。組織全体のデータが統一形式で表示されるため、より効率的なデータの収集、分析、および対応が可能になります。</p> <p>Eventia Suiteは、すべてのチェック・ポイント製品および多種多様なサードパーティ製品で記録されたログとイベント・アクティビティについて、収集、監査、相関分析、およびレポートリングを行います。Eventia Reporterは、各種の情報を収集し、複数の製品にまたがる攻撃、ブロックしたトラフィック、ログイン・アクティビティ、およびネットワーク・アクティビティについてレポートリングします。Eventia Reporterのエンドポイント・セキュリティ・レポートでは、ポリシー違反に関するIntegrityデータ、ファイアウォール・イベント、ブロックしたプログラム、Integrity MailSafe™ イベント、スパイウェア、Malicious Code Protectorの結果、およびクライアント・エラーに関する統一レポートが提供されます。Eventia Reporterは、アンチウイルス・アクティビティ、Connectra、InterSpect、およびVPN-1 Power VSXのログ・レポートについてのレポートも提供します。</p> <p>Eventia Suiteでは、カード会員情報へのユーザ・アクセス、管理者が行った操作、無効な論理的アクセスの試みなどについての監査証跡を記録することができます。Eventia Analyzerは、監査ログの初期化と監査情報への安全なアクセスをサポートし、システム・レベル・オブジェクトの作成と削除にも対応しています。また、監査ログが初期化されたときや、システム・オブジェクトが作成または削除されたときにアラートを生成することもできます。</p> <p>チェック・ポイントのユーザ認証機能およびロギング機能により、システム・イベントを再現および分析するための監査証跡の確保が可能になります。</p>

要件	チェック・ポイントのソリューション
<p>10.3 各システム・コンポーネントで発生した各イベントについて、少なくとも次の監査証跡を記録する。</p> <ul style="list-style-type: none"> ● ユーザの識別子 ● イベントの種類 ● イベントが発生した日時 ● イベントが成功したか失敗したか ● イベントの起点 ● 影響を受けたデータ、システム・コンポーネント、およびリソースの識別子または名前 	<p>チェック・ポイントのすべてのソリューションでは、チェック・ポイントのゲートウェイを通過したトラフィックにおけるユーザおよび管理者のアクティビティを詳細にロギングおよび追跡することができます。この機能では、送信元/送信先およびアドレス / サービス、認証されたユーザ、日時、操作、関係するチェック・ポイントのソリューションなど、この条項の要件を満たすために必要なすべての情報が提供されます。この情報は、SmartViewTracker、またはEventia Reporterのレポートで確認できます。Eventia Reporterでは、ロギングされたその他の情報を記録することもできます。また、機能拡張によって、標準では対応していないログ形式を扱うことも可能になります。</p>
<p>10.4 すべての重要なシステムの時刻を実際の時刻に同期させる。</p>	<p>チェック・ポイントのソリューションでは、NTP (Network Time Protocol) などの標準の時刻同期プロトコルを使用して、すべてのシステムの時刻を実際の時刻に同期させることができます。</p>
<p>10.5 監査証跡が改編されないように保護する。</p>	<p>監査証跡に関するセキュリティ機能は、すべてのチェック・ポイント製品で共通です。この機能では、ログ・サーバへのトラフィックの暗号化、ログの分散保存、フォレンジック・データのグラフィカルな検索、ログ・ローテーション / アーカイブのためのツールおよびポリシー、Eventia Analyzerとの統合によるイベントの相関分析と検出、Eventia Reporterとの統合による傾向分析とレポート生成、OPSECパートナーのサードパーティ・ツールに対するLEA / ELAサポート、無償のOPSEC SDKで開発されたカスタム・ツールに対するLEA / ELAサポートなどが提供されます。</p> <p>監査証跡を表示するには、管理者でもログインが必要です。チェック・ポイント製品は管理権限の委譲をサポートしており、管理者プロファイルにおいて、ログおよび監査証跡に対する読み取り / 書き込み権限を付与するかどうかを明示的に指定することができます。</p> <p>Eventia Reporterでは、ログへのアクセスとその改変を困難にするオフライン・ログを生成することができます。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、チェック・ポイント製品によるロギングを適切に設定し、保存されたログ・データの完全性を維持するためのコンサルティング・サービスを提供しています。</p>

要件	チェック・ポイントのソリューション
<p>10.6 すべてのシステム・コンポーネントのログを少なくとも1日1回チェックする。ログ・チェックでは、侵入検知 (IDS) などのセキュリティ機能を提供するサーバや、認証 / 認可 / アカウンティング (AAA) プロトコル・サーバ (RADIUS など) を対象とする必要がある。</p>	<p>第10.6項で規定されているログ・チェックの必須プロセスは、チェック・ポイントのロギング・システムで対応することができます。Eventia Suiteでは、広範なシステム・コンポーネント(チェック・ポイントのすべての製品と著名なサードパーティ製品)のログを定期的にチェックすることが可能で、管理者は、セキュリティ・プラクティスに定められた頻度でログをチェックできます。Eventia Analyzerでは、集中管理コンソールを使用して、ログとイベントの相関分析を効率的に行うことができます。ログのチェック、分析、およびレポートの一元化によって、セキュリティ・アクティビティおよびネットワーク・アクティビティの全体的な傾向を把握することが可能となっています。</p>
<p>10.7 監査証拠の履歴は、少なくとも1年間は保存し、少なくとも3か月はオンラインで参照できるようにする。</p>	<p>チェック・ポイントの管理ソリューションが収集した監査証拠は、自動的にエクスポートして、指定した期間だけ保存しておくことができます。Eventia Reporterを使用すると、ログをオフライン・ログとして管理することができます。ログ・ファイルは元の形式で管理し、必要に応じてEventia Reporterに再ロードすることが可能です。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、データ(チェック・ポイントのソリューションによって生成された監査証拠を含む)の適切な保存手順を策定するためのコンサルティング・サービスを提供しています。</p>

要件	チェック・ポイントのソリューション
<p>11. セキュリティ・システムおよびセキュリティ・プロセスを定期的に検査する</p>	
<p>11.1～11.3 これらの条項は、セキュリティ制御および接続のテスト、脆弱性スキャンの実行、侵入テストの実行に関する要件です。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、チェック・ポイントのソリューションが、第11.1～11.3項で規定されているとおりに適切に導入されているかどうかを検証するテストおよびスキャンを実施するためのコンサルティング・サービスを提供しています。</p>	
<p>11.4 ネットワーク侵入検知システム、ホスト・ベースの侵入検知システム、および侵入防御システムを使用して、すべてのネットワーク・トラフィックを監視し、セキュリティ侵害の可能性があれば担当者に通知する。</p> <p>すべての侵入検知 / 侵入防御エンジンを常に最新の状態で維持する。</p>	<p>SmartDefenseとWeb Intelligence技術は、Connectra、Integrity、およびVPN-1の一部として侵入防御機能を提供します。</p> <p>Eventia Suiteは、ネットワーク・トラフィックを監視し、不審なアクティビティやセキュリティ侵害の可能性が見つかった場合に担当者に通知します。Eventia Analyzerは、イベントの相関分析を行うことにより、複数のデバイスにまたがる複雑で発見が困難なセキュリティ・インシデントを検出し、被害の拡大を抑制します。</p> <p>SmartDefenseサービスにより、侵入防御エンジンを常に最新の状態で維持することが可能になります。</p>
<p>11.5 ファイルの完全性を監視するソフトウェアを導入し、重要なシステムやコンテンツ・ファイルの改ざんが見つかった場合に担当者に通知する。</p> <p>また、重要なファイルの比較を週に1回以上実行するようソフトウェアを設定する。</p>	<p>Integrityは、ネットワーク・アクセスを行うすべてのアプリケーションのリストを作成し、MD5ハッシュ値を収集します。管理者は、これらを使用してアプリケーションが改ざんされていないかどうかを確認できます。またIntegrityは、新しいアプリケーションや許可されていないアプリケーションが見つかった場合に管理者に通知します。管理者は、不正アクセスの試みに対してアクションを実行するためのルールを設定することができます。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、チェック・ポイントのソリューションでは直接カバーすることのできない、ファイルの完全性の監視を行うためのコンサルティング・サービスを提供しています。</p>
<p>12. 従業員および契約業者向けの情報セキュリティに関するポリシーを策定し、運用する</p>	
<p>管理ポリシーの策定に関するこの要件は、チェック・ポイントのソリューションで直接満たすことはできません。</p> <p>チェック・ポイントの認定代理店、システム・インテグレータ、および販売代理店は、第12項で規定されているプロセスおよび手順を策定、実装するためのコンサルティング・サービスを提供しています。</p>	

まとめ

ペイメント・カード情報を取り扱う組織にとって、データ詐欺の脅威もPCI規格も当面は避けて通ることのできない課題です。PCI規格準拠の達成率は、これまでのところ予想を下回る結果となっていますが、大多数の企業は、規格への準拠は現在の最優先課題であるとしています。PCI規格に準拠することは、単に罰金を科せられないようにするためだけでなく、安定した企業運営を行うためにも重要なことです。つまり、PCI規格に準拠することで、リスクを軽減し、より多くのチャネルでサービスを提供し、さらには顧客およびビジネス・パートナーの信頼を維持することが可能になるのです。またPCI規格に準拠することは、それ以外の法規制や業界標準を遵守する取り組みの一助にもなります。チェック・ポイントは、組織のセキュリティ基盤を構築するための包括的な手段として、PCI規格の大半の要件に対応する、統合された数々のソリューションを提供しています。加盟店、金融機関、そして情報処理業者は、チェック・ポイントのソリューションを使用することで、顧客からの信用と信頼を守ることが可能になります。

付録：PCI規格準拠に関するチェック・ポイント製品

チェック・ポイントの境界セキュリティ・ソリューション

VPN-1 Power

VPN-1 Powerは、ファイアウォール、VPN、および侵入防御の各機能が緊密に統合されたゲートウェイ製品で、ミッション・クリティカルな環境向けにハイ・パフォーマンスなセキュリティを提供します。

VPN-1 UTM

VPN-1 UTMは、あらゆる規模の企業に対応する拡張性を備えた統合脅威管理ソリューションです。実績ある各種のセキュリティ機能を単一のソリューションとして提供することにより、セキュリティ環境の簡素化を可能にします。VPN-1 UTMでは、ファイアウォール、侵入防御、アンチウイルス、アンチスパイウェア、Webアプリケーション・ファイアウォール、IPSec VPN、およびSSL VPNの各機能が、容易に管理可能な1つのソリューションに完全統合されています。

UTM-1

UTM-1は、ファイアウォール、VPN、アンチウイルス、および侵入防御などVPN-1 Power/VPN-1 UTMで既に多数実績のある各セキュリティ機能を緊密に統合したUTMアプライアンスで、大企業の中規模支店、支店環境や、中規模企業の拠点などの管理者が存在しないネットワーク環境における総合的なセキュリティをオールイン・ワンで提供します。

VPN-1 UTM Edge

VPN-1 UTM Edgeは、ファイアウォール、VPN、侵入防御、およびアンチウイルスの各機能が統合された、支社・支店環境向けのゲートウェイ・アプライアンスです。VPN-1 UTMやVPN-1 Powerと共に容易に管理可能なVPN-1 UTM Edgeにより、リモート・サイト環境にネットワーク・サービスを提供しながら、組織全体にわたって一貫性のあるセキュリティ・ポリシーを実施することが可能になります。

VPN-1 SecureClient

モバイル環境で業務を行う社員が増加したことに伴い、企業リソースへの安全なリモート・アクセスやリモートPCの保護といった重要なセキュリティ上の課題に対処できる優れたVPNソリューションが求められるようになってきました。VPN-1 SecureClientは、UTM-1、VPN-1 UTM、VPN-1 UTM Power、VPN-1 Powerゲートウェイに接続するための、あらゆるネットワーク環境のニーズを満たすVPNクライアント製品です。VPN-1 SecureClientは、IPSecによる暗号化とデータの認証を行うことで、リモート・アクセス時における盗聴やデータの改ざんを防止します。さらに、PCのセキュリティ・ポリシーをリモート・ユーザにも適用できるようにすることで、社内PCと同じレベルのセキュリティをリモートPCでも実現します。

チェック・ポイントの内部セキュリティ・ソリューション

InterSpect

InterSpectは、ワームやサービス妨害 (DoS) 攻撃、電子メール経由で広まるマルウェアなど、ネットワーク内部の脅威に対する防御機能を提供します。InterSpectは、内部ネットワーク固有の要件を満たすように独自設計された侵入防御機能、ネットワーク・ゾーンのセグメント化機能、およびホストの隔離機能を備えています。例えば、セキュリティ対策が不十分なPCによるネットワーク・アクセスのブロック、Citrix ICAやMicrosoft SQLなどのLANプロトコルの包括的な保護、SQLインジェクションやバッファ・オーバーフロー攻撃のブロックといった機能が提供されます。ネットワーク接続されたすべてのPCを保護し、ネットワーク・アクセス・ポリシーを確実に実施することによって企業のセキュリティを強化するInterSpectは、チェック・ポイントのTotal Access Protection (総合的なアクセス保護) 構想において重要な役割を果たしています。

チェック・ポイントのWebソリューション

Connectra

Connectraは、SSL VPNアクセス機能と、統合されたエンドポイント・セキュリティおよびアプリケーション・セキュリティを単一の統合ソリューションとして提供する包括的なWebセキュリティ・ゲートウェイです。接続機能とセキュリティの両方を単一のソリューションに搭載したことで、SSL VPNアクセスを効率よく安全に多様なユーザーに提供することを可能にしています。

Web Intelligence

Web Intelligenceは、Web環境全体に対する包括な防御機能を提供するWebアプリケーション・ファイアウォール技術です。Web Intelligenceは、Connectra、VPN-1 Power、UTM-1、VPN-1 UTM Edge、およびVPN-1 UTMでサポートされており、その背後にあるネットワーク、オペレーティング・システム、Webサーバ、およびバックエンド・システムのためのマルチレイヤの防御機能を提供します。Web Intelligenceは、防御機能のアップデートおよび設定アドバイザリをリアルタイムで提供するSmartDefenseサービスを通じて、最新の脅威にも対応します。

SSL Network Extender

SSL Network Extenderは、クライアントレスのリモート・アクセス機能と、IPベースのあらゆるアプリケーションに対する完全なネットワーク接続機能を提供するブラウザ・プラグインです。SSL Network Extenderは、VPN-1ゲートウェイのIPSec VPN機能にSSL VPN機能を追加することにより、リモート・アクセス環境を簡素化すると同時に、あらゆるリモート・アクセス・シナリオを可能にする最大限の柔軟性をもたらします。SSL Network ExtenderはConnectraでも使用できます。

チェック・ポイントのエンドポイント・セキュリティ・ソリューション

Integrity

Integrityは、内部ネットワークのエンドポイントPCを保護するための管理性に優れた包括的な統合ソリューションです。Integrityは、LANを停止させ、業務を混乱させる可能性のある最新のワームやスパイウェア、ハッカーの攻撃をブロックします。また、ネットワークへの接続を許可する前に、すべてのPCにアンチウイルスやパッチなどの要件を遵守させます。Integrityを他のチェック・ポイント製品と組み合わせることにより、Total Access Protectionを実現することが可能になります。

Integrity IM Security

Integrity IM Securityは、インスタント・メッセージング (IM) による通信の機密性と安全性を維持する、あらゆるIMサービスに対応した包括的なIMセキュリティ・ソリューションです。IM SecurityはIntegrityにシームレスに統合され、ポリシー・ベースのエンドポイント・セキュリティ、メッセージの暗号化機能、およびプロトコル・レベルの防御機能を提供します。これにより、サーバやゲートウェイを別途導入することなく、包括的なIMセキュリティが実現され、スパマー、ソーシャル・エンジニアリング攻撃、ハッカー、および脆弱なIM接続を突くマルウェアからエンドポイントPCを保護することが可能になります。

Integrity Anti-Spyware

Integrityエンドポイント・セキュリティ・スイートの統合モジュールであるIntegrity Anti-Spywareは、アンチスパイウェア・セキュリティの管理を簡素化し、単一のクライアント・セキュリティ環境を実現します。Integrityに統合されたIntegrity Anti-Spywareモジュールは、Integrityサーバから管理することが可能です。Integrity Anti-Spywareは、トロイの木馬やキーロガーなどのスパイウェアを検出、隔離、および除去します。

チェック・ポイントのセキュリティ管理ソリューション

SmartCenter

SmartCenterソリューション群は、チェック・ポイントの統一セキュリティ・アーキテクチャに基づいており、単一の統合コンソールからあらゆるセキュリティ管理作業を行えるようにします。例えば、セキュリティ・ポリシーおよびセキュリティ・アクティビティの集中管理や、防御機能に対するアップデートの一括配布を行うことができます。この包括的なアプローチにより、組織全体にわたって一貫性のあるポリシーを実施して、重要な企業資産を保護すると共にセキュリティ投資効果の最大化を図ることが可能になります。SmartCenterソリューション群は、チェック・ポイントの境界、内部、Web、およびエンドポイント向けのセキュリティ製品をサポートしています。

Eventia Analyzer

Eventia Analyzerは、チェック・ポイントのセキュリティ・ゲートウェイおよびサードパーティ・デバイスで発生したセキュリティ・イベントの相関分析および管理を一元的かつリアルタイムに行うためのソリューションです。データの集約と相関分析を自動化することにより、データの分析に必要な時間を大幅に短縮できるほか、真のセキュリティ上の脅威を顕在化させて、その問題への対応を優先的に行うことが可能になります。

Eventia Reporter

Eventia Reporterは、セキュリティ・デバイスおよびネットワーク・デバイスから収集された膨大な量のデータを意味のある情報に変換し、事前定義されたレポートまたはカスタマイズ・レポートを生成します。このレポートは、セキュリティ・ポリシーやセキュリティ対策の実効性を検証したり必要なネットワーク・キャパシティを予測したりするのに利用できるほか、セキュリティ投資効果を最大化するためにも役立ちます。

Check Point Software Technologies Ltd.について

チェック・ポイント・ソフトウェア・テクノロジーズ・リミテッド (www.checkpoint.com) はインターネット・セキュリティにおけるトップ企業として、世界中の企業向けファイアウォール、パーソナル・ファイアウォール、データ・セキュリティおよびVPN市場においてマーケット・リーダーとして広く認められています。チェック・ポイントは、ネットワーク・セキュリティ、データ・セキュリティ、およびセキュリティ管理ソリューションを含む広範囲なポートフォリオにより、ITセキュリティへのPUREなフォーカスを実現します。チェック・ポイントは、NGXプラットフォームを通じて、企業ネットワークおよびアプリケーション、リモート・ユーザ、支店・支社環境、およびパートナー各社のエクストラネットのビジネス通信およびリソースに対する広範なセキュリティ保護を実現する、統一されたセキュリティ・アーキテクチャを提供しています。更にチェック・ポイントは、業界をリードするデータ・セキュリティ・ソリューションである、PointSec製品ラインナップを通じ、PCやモバイル端末に保存してある各種企業データや重要なデータの暗号化と保護を提供します。数々の受賞歴のあるチェック・ポイントのZoneAlarm Internet Security Suiteとその他のコンシューマ向けセキュリティ・ソリューションは、世界中で何百万にも及ぶお客様のPCをハッカー、スパイウェア、および情報窃盗から未然に保護しています。またチェック・ポイントは、350社を超える各分野のトップベンダーが提供する“ベスト・オブ・ブリード”ソリューションとの統合および相互運用性を実現するフレームワークであるOPSEC (Open Platform for Security)により、自社ソリューションの能力をさらに拡大します。現在、チェック・ポイント・ソリューションは、世界中のパートナー・ネットワークを通じて販売、導入、サービス提供されています。チェック・ポイントの顧客には、Fortune 100社の全社と何万ものあらゆる規模の企業や組織が含まれています。

©2003-2007 Check Point Software Technologies Ltd. All rights reserved.

Check Point, Application Intelligence, Check Point Express, Check Point Express Cl, Check Pointのロゴ, AlertAdvisor, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Sentivist, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express Cl, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, Zone Labsのロゴは、Check Point Software Technologies Ltd. あるいはその関連会社の商標または登録商標です。ZoneAlarm is a Check Point Software Technologies, Inc. Company. その他の企業、製品名は各企業が所有する商標または登録商標です。本書で記載された製品は米国の特許No.5,606,668、5,835,726、6,496,935、6,873,988、および6,850,943により保護されています。その他の米国における特許や他の国における特許で保護されているか、出願中の可能性があります。

Building a Foundation for PCI

P/N:502340-J 2007.05

*記載された製品仕様は予告無く変更される場合があります。



Check Point[®]
SOFTWARE TECHNOLOGIES LTD.

チェック・ポイント・ソフトウェア・テクノロジーズ株式会社
〒160-0022 東京都新宿区新宿5-5-3 建成新宿ビル6F
<http://www.checkpoint.co.jp/> E-mail: info_jp@checkpoint.com Tel: 03 (5367) 2500