



## PCI規格の遵守：エンドポイントに保存された カード会員情報の保護

チェック・ポイントのソリューションで実現する、  
小売環境のエンドポイントに保存されたデータの保護

# Contents

本書の内容

概要 .....	3
幅広いセキュリティ要件が規定されたPCI規格 .....	4
PCI要件3：保存されたカード会員情報の保護 .....	5
エンドポイント上のデータを保護する手段 .....	6
小売環境におけるPCI遵守を可能にするチェック・ポイント製品 .....	8

## 概要

Payment Card Industry Data Security Standard (PCI DSS) は、カード会員情報を保護するための制度的な仕組みです。元々はVisaとMasterCard Internationalが共同で策定したのですが、現在ではすべての大手国際ペイメント・カード会社が参加しており、事実上の業界標準となっています。PCI規格は、6つの統制目標と12の要件から構成されています。PCI規格の要件が定める範囲は幅広く、ネットワーク・セキュリティと情報セキュリティに関するほとんどすべての要素が網羅されています。各要件は、セキュリティ技術と最も効果的な方法により構成されています。要件を遵守しているかどうかの検証方法と関連する監査手順は、小売業者およびカード決済に関与する他の組織が取り扱う取引件数によって異なります。

現在、PCI規格などの規定を遵守することは小売業界にとって重要な問題となっています。数百万人もの被害者を出している最近のデータ侵害事件によって、消費者がこうした問題に厳しい目を向けるようになってきているからです。PCI規格を遵守できていない場合、実際にデータ侵害が発生するだけでなく、顧客や取引先の信頼を失い、情報漏洩に対する補償費用や顧客への通知費用が発生し、場合によっては民事責任を問われる可能性があります。さらに、PCI規格が業界全体で採用されたことにより、これを遵守していなかった場合にはクレジット・カードを一切取り扱えなくなるおそれもあります。これはつまり、消費者が最も多く使用する決済手段を受け付けられなくなるということです。

PCI規格にはほぼすべてのセキュリティ技術と最も効果的な方法が網羅されているため、その遵守に取り組むにあたっては、各要件に優先順位を付け、最も優先度の高いものから着手する必要があります。最終的な目標はカード会員情報を保護することであり、これこそがPCI規格の使命です。この技術白書では、PCI規格について概説し、データ保護のための要件を検証して、データを安全に保存するための必要事項を示します。またフルディスク暗号化やポート管理などの技術的手段についても取り上げ、主にエンドポイント・デバイス（ノートPCやPDA、スマートフォン、USBストレージ・デバイスなど）において、これらがPCI規格を遵守するうえでどのように役立つのかを解説します。本書は、PCI規格の特定の条項およびそのセキュリティ監査手順を遵守するためにどのようなセキュリティ・ソリューションを使用すればよいかを、各小売環境において適切に判断できるようにすることを目的としています。

## 幅広いセキュリティ要件が規定されたPCI規格

### Payment Card Industry Data Security Standard

Payment Card Industry Data Security Standard (PCI DSS) は、ネットワーク、アプリケーション、およびカード会員情報を保護するための6つの統制目標とそれを支える12の要件で構成されています。PCI規格を遵守するためには、広範なセキュリティ技術と最も効果的な対策を用いる必要がありますが、これはいずれも特殊なものではありません。PCI規格の要件は、情報セキュリティに関する多くの法律や規制、最も効果的なポリシーと似ています。小売業者は、PCI規格の幅広い規定に従うことで、重要なビジネス・システムおよび業務の機密性、完全性、可用性を維持するために、考えられる限り最良の対策を講じたことになります。PCI規格では、小売業者は次のことを実施するように規定されています<sup>1</sup>。

#### 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て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・ソフトウェアを導入して定期的に更新する
- (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て保守する。

#### 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。

#### PCI規格の要件に対応するチェック・ポイント製品

ネットワーク・セキュリティ	データ・セキュリティ	セキュリティ管理
● ファイアウォール/VPN	● フルディスク暗号化とアクセス制御	● 監視およびレポートのための集中プラットフォーム
● 統合脅威管理 (UTM)	● モバイル・デバイス暗号化	● セキュリティ管理ポータル
● 侵入検知/侵入防御	● ポート管理とリムーバブル・メディア暗号化	
● エンドポイント・セキュリティ		

1: PCIバージョン1.1 (2006年9月); [https://www.pcisecuritystandards.org/pdfs/pci\\_dss\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf)

## PCI要件3： 保存されたカード会員情報の保護

PCI要件3.4は、保存されたデータの保護に関するいくつかの条項の中でも特に重要な要件です。要件3.4では、カード番号 (Primary Account Number: PAN) を保護するように定められています。またPANと共に、カード会員名、サービス・コード、および有効期限を保存する場合は、これらも保護する必要がありますとされています。この技術白書では主に、保存されたデータの保護に関するPCIの規定を、要件3.4で定められているとおりに遵守する方法について解説しています。

データを保存する際は、セキュリティ管理の手段を用いて、権限のある人物以外は絶対に機密情報へアクセスできないようにする必要があります。具体的には、権限がなければデータを読み取れない/使用できない状態にします。要件3には、「カード会員情報を保護するには暗号化を行うことが極めて重要である」と記述されています。さらに、「潜在的なリスクを軽減するため、保存されたデータを保護するその他の有効な手段についても検討するべきである」とされています。このように規定されている理由は、保存されたデータに対する各種のリスクに対しては、暗号化以外のソリューションが有効な場合もあるからです。小売環境には、カード会員情報に不正アクセスできる機会が溢れています (以下の「小売環境のエンドポイントを保護するうえでの課題」を参照)。したがって、要件3.4を確実に遵守するためには、各環境に存在するリスクを慎重に評価することが重要となります。

### 小売環境のエンドポイントを保護する上での課題

小売業では、本部や各支店、配送センター、店舗にそれぞれ独自のソリューションが導入されており、そのIT環境を保護することは容易ではありません。また保有店舗数が数百から数千にも及ぶ大規模業者の場合、店員が最小限のITスキルしか持っていない、技術担当者が店舗にごくわずかもしくは全くいない、という状況で数多くのエンドポイントを保護する必要があるため、さらなる困難に直面することになります。

#### エンドポイントからのPCI関連データの漏洩を防ぐには

支払い処理に使用されるエンドポイントPCやモバイル・デバイスを保護することは、PCI関連データの漏洩を防ぐことにつながります。POSアプリケーションに記録されたクレジット・カードの決済情報は、多くの場合、中央サーバだけでなくローカルのエンドポイントにも保存されます。特に、フランチャイズ店や、加盟店銀行 (カード加盟店の決済処理を行う銀行) との通信のためにデータをローカルに保存する必要のあるレガシー・システムではこのような仕組みになっているのが一般的です。そのため、雑然とした状況に陥りやすい小売店では、エンドポイントに保存されたPCI関連データを自動的、透過的、そして包括的に保護することのできるセキュリティ・ソリューションが必要となります。PCI規格では、PANおよび関連データを、権限のある人物以外は読み取れない状態にすることが求められます。また、モバイル・デバイスを保護すると共に、許可されていないモバイル・ストレージ・デバイスへのデータ・コピーを行えないようにすることも必要です。

## 要件3.4： PANを読み取り不可能な状態にする

PCI要件3.4では、次のように定められています。

PANの保存先では、以下のいずれかの手段を用いて少なくともこれを読み取り不可能な状態にする (持ち運び可能なデジタル・メディア、バックアップ・メディア、ログに保存する場合、無線ネットワーク経由で保存する場合を含む)。

- 強固な一方向性ハッシュ関数 (ハッシュ・インデックス)
- 一部情報の切り捨て
- インデックス・トークン、PAD (PADは安全に保存する)
- 強固な暗号 (鍵管理のプロセスおよび手順を定める)

## 暗号化技術の使用によるPCI規格の遵守

暗号化とは、平文のデータを、特定の知識または権限を持つ人物以外は読み取れない状態にするプロセスのことを言います。保存されたデータを暗号化する技術には、ファイル・レベルの暗号化、カラム・レベルの暗号化、そしてディスク・レベルの暗号化（フルディスク暗号化）があります。要件3.4.1では、フルディスク暗号化について次のように定められています。

ファイル・レベルの暗号化やデータベースのカラム・レベルの暗号化ではなく、ディスク暗号化を使用する場合、その論理的アクセスは、オペレーティング・システム自体が備えるアクセス制御メカニズムからは独立したメカニズムで管理する必要がある（例えば、ローカル・システム・アカウントやActive Directoryアカウントを使用してはならない）。復号鍵をユーザ・アカウントに関連付けてはならない。

## テスト手順

要件3.4.1を遵守できているかどうかをテストするため、PCI Security Standards Councilでは、「PCIセキュリティ監査手順<sup>2</sup>」の条項3.4.1.a～3.4.1.cで次のようにテスト手順を定めています。

3.4.1.a ディスク暗号化を使用している場合は、暗号化されたファイル・システムへの論理的アクセスが、オペレーティング・システム自体が備えるメカニズムからは独立したメカニズムに基づいて行われていることを確認する（例えば、ローカル・アカウントやActive Directoryアカウントを使用してはならない）。

3.4.1.b 復号鍵がローカル・システムに保存されていないことを確認する（例えば、フロッピー・ディスクやCD-ROMに安全な形で保存し、必要なときにだけ取り出せるようにする）。

3.4.1.c リムーバブル・メディアに保存されたカード会員情報が常に暗号化されていることを確認する（ディスク暗号化ではリムーバブル・メディアを暗号化できない場合が多い）。

なお要件3.4では、何らかの理由によりカード会員情報を暗号化できない場合は、付録B「保存されたデータの暗号化に対する代替手段」を参照するよう記述されています。

## エンドポイント上のデータを保護する手段

PCI規格では、その規定を遵守するために使用するべき暗号化技術は指定されていません（「3-DES（128ビット）やAES（256ビット）などの強固な暗号化技術を使用し、鍵管理のプロセスと手順を定める」とされています）。実際、年1回実施する必要がある自己診断の項目3.5でも、「（データベースやログ、ファイル、バックアップ・メディアなどに保存された）カード番号は、暗号化や一部情報の切り捨てといった方法を用いて安全に保存されているか<sup>3</sup>」としか書かれていません。またそれに対して用意されている回答も、「はい」と「いいえ」だけです。

## ファイル/フォルダ・レベルの暗号化とフルディスク暗号化

ファイル/フォルダ・レベルの暗号化は、ストレージ・デバイス上の特定ファイルまたは特定フォルダのデータを保護するために使用します。ファイル/フォルダ・レベルの暗号化のメリットは処理の速さです。特定のデータだけを暗号化するため、そのぶんアクセスが高速になります。これは特に、数十万から数百万単位のカード会員の決済処理を行うサーバにおいて重要なことです。

2： [https://www.pcisecuritystandards.org/pdfs/pci\\_audit\\_procedures\\_v1-1.pdf](https://www.pcisecuritystandards.org/pdfs/pci_audit_procedures_v1-1.pdf)を参照

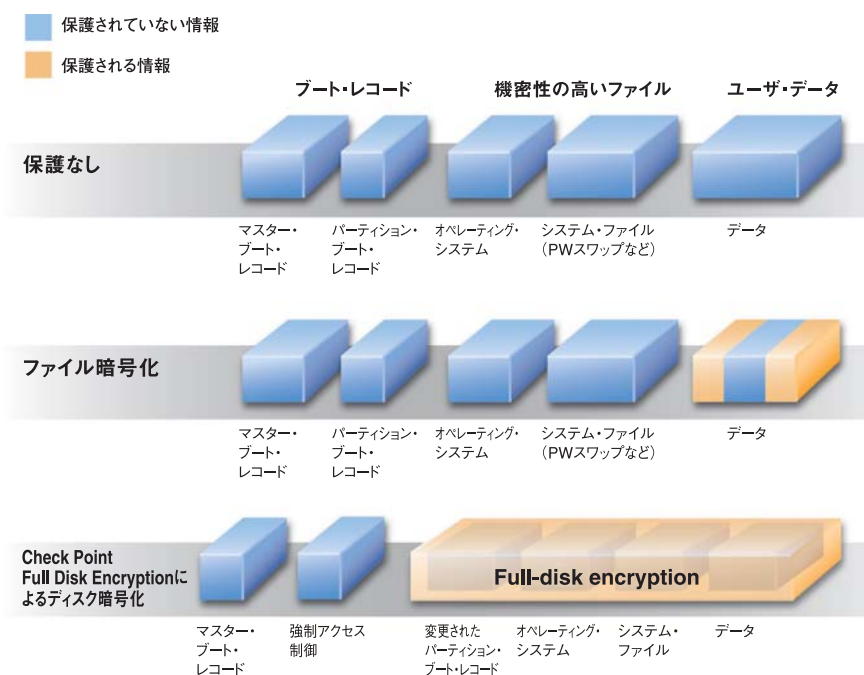
3： [https://www.pcisecuritystandards.org/pdfs/pci\\_saq\\_v1-0.pdf](https://www.pcisecuritystandards.org/pdfs/pci_saq_v1-0.pdf)を参照

一方エンドポイント・デバイスの場合、デバイス上のコンテンツ全体を自動的に保護できるフルディスク暗号化が適しています。保存場所やアプリケーションの種類、保存形式を問わず、デバイス上のすべてのPANおよび関連データが保護されるため、デバイスを紛失したり盗まれたりした場合でもPCI違反を問われる可能性は最小限に抑えられます。対象のファイルやフォルダをユーザが指定する必要のあるファイル / フォルダ・レベルの暗号化とは異なり、フルディスク暗号化では自動的に暗号化が行われます。そのため、保存データのセキュリティに関するPCI規格の要件も自動的に満たすことができます。

またパフォーマンスについても、チェック・ポイントのフルディスク暗号化製品Check Point Endpoint Security™ Full Disk Encryptionが稼働しているエンドポイント・コンピュータは、企業における典型的な使用条件であれば、暗号化されていない場合の95%~98.5%のパフォーマンス・レベルで動作することが確認されています（パフォーマンス測定ソフトウェアPassMarkでのテストによる）。すべてのデータが自動的にかつ完全に保護されるというメリットを考えると、この程度のパフォーマンス低下は大きな問題にはなりません。

### 暗号化プロセスの比較：ファイル / フォルダ・レベルとフルディスク

PANおよび関連データが保存されたエンドポイントが保護されていない場合、そのデバイスにアクセスできるユーザは誰でもこれらの情報にアクセスできてしまいます。ファイル / フォルダ・レベルの暗号化で保護されるのは、ストレージ・デバイス上の指定された場所に保存されているデータだけです。場所を限定した暗号化の場合、仮想メモリや一時ディレクトリにシステム・ファイル、アプリケーション・ファイルとして存在しているPANおよび関連データのコピーに許可なくアクセスされる可能性があります。これらのファイルは、ファイル/フォルダ・レベルの暗号化では保護することができないため、PCI違反となる可能性があります。



Check Point Endpoint Security Full Disk Encryptionは、エンドポイント上のすべてのPCI関連データを保護します。

#### 4: チェック・ポイントのレポート「暗号化がディスク・パフォーマンスに与える影響の検証」

「フルディスク暗号化は、小売環境のエンドポイント・デバイスに保存されたPANおよび関連データを、PCI規格に準じて保護するための実践的かつ効果的な手段です」

Alan Phillips氏

7Safe Ltd.

PCI DSS認定評価担当者

Check Point Full Disk Encryptionによるフルディスク暗号化は、マスター・ブート・レコードおよび強制アクセス制御の段階から処理が始まります。このドライバ・ベースの「起動前」認証プロセスを行わない場合、ディスク全体へのアクセスがブロックされ、マシンは起動しません。Check Point Full Disk Encryptionは、システム起動後はバックグラウンドで動作するため、ディスク上のすべてのコンテンツ（一時システム・ファイルを含むすべてのデータ）は常に自動的に暗号化されます。エンドポイント・コンピュータがスタンバイ状態またはハイパネーション状態になるか、シャットダウンした後、再度デバイスにアクセスするには、認証を受け直す必要があります。

### 小売環境のエンドポイントに保存されたデータの保護に関するその他の問題

ANおよび関連データが漏洩する可能性があるのは、デスクトップPCやノートPCからだけではありません。小売店での売上処理に使用されるネットワーク・デバイスや、Symbian、Pocket PC、Windows Mobile Smartphone、Palmといったオペレーティング・システムを搭載するモバイル・デバイス（PDAやスマートフォンなど）も漏洩元になる可能性があります。PCI遵守のための包括的な暗号化戦略では、データを保存することのできるモバイル・デバイスも考慮に入れる必要があります。

またデータ漏洩を防ぐためには、USBポートなどに接続されたモバイル・ストレージ・デバイスへのPCI関連データのコピーも制御する必要があります。USBフラッシュ・ドライブやiPod、デジタル・カメラ、Bluetoothデバイスなどがこれに該当します。これらのデバイスを適切に制御していない場合、保護すべきデータが許可なくモバイル・ストレージ・デバイスにコピーされ、PCI違反となる可能性があります。

### 小売環境におけるPCI遵守を可能にするチェック・ポイント製品

チェック・ポイントは、PCI要件3「保存されたカード会員情報の保護」の遵守を可能にする3つのデータ・セキュリティ・ソリューションを提供しています。Check Point Full Disk EncryptionはデスクトップPCおよびノートPC向けのデータ・セキュリティ機能を、Pointsec MobileはPDAやスマートフォン向けの暗号化機能を、そしてCheck Point Endpoint Security Media Encryptionはデータ漏洩防止機能とリムーバブル・メディアの暗号化機能をそれぞれ提供します。これら3つの製品を組み合わせることにより、小売環境のエンドポイントに保存されたデータに対する主要なリスクに対処できるようになります。

#### 保存されたカード会員情報を保護するチェック・ポイントのソリューション

##### Check Point Full Disk Encryption

強力なフルディスク暗号化機能とアクセス制御機能を提供します。小売環境向けPCデータ・セキュリティの集中管理機能も提供するCheck Point Full Disk Encryptionは、LinuxおよびWindowsで動作し、最高レベルの認定のほとんどを取得しています。

##### Pointsec Mobile

内蔵ストレージおよびメモリ・カード上のファイルを暗号化することによって、Symbian、Pocket PC、Windows Mobile Smartphone、およびPalmオペレーティング・システム（プラットフォーム）搭載デバイス上のPCI関連データを包括的に保護します。

##### Check Point Media Encryption

ポート管理、コンテンツ・フィルタリング、オプションのメディア暗号化などの機能により、ポートとストレージ・デバイスの包括的な管理を可能にし、企業内のデスクトップPCやノートPCに保存されている機密情報の不正なコピーを防ぎます。

## PCI要件3.4の遵守

チェック・ポイントの暗号化技術は、デスクトップPCやノートPC、モバイル・デバイスといった小売環境のエンドポイント上にあるPANおよび関連データを、その保存場所に関係なく完全に読み取り不可能な状態にすることができます。起動前認証機能を備えるチェック・ポイントのフルディスク暗号化技術は、いったん導入すればその後は特別な操作や設定を行うことなく、各エンドポイント上で自動的かつ透過的に動作します。また、強固な認証、ポリシーの集中管理、鍵の復元といった機能も備えています。

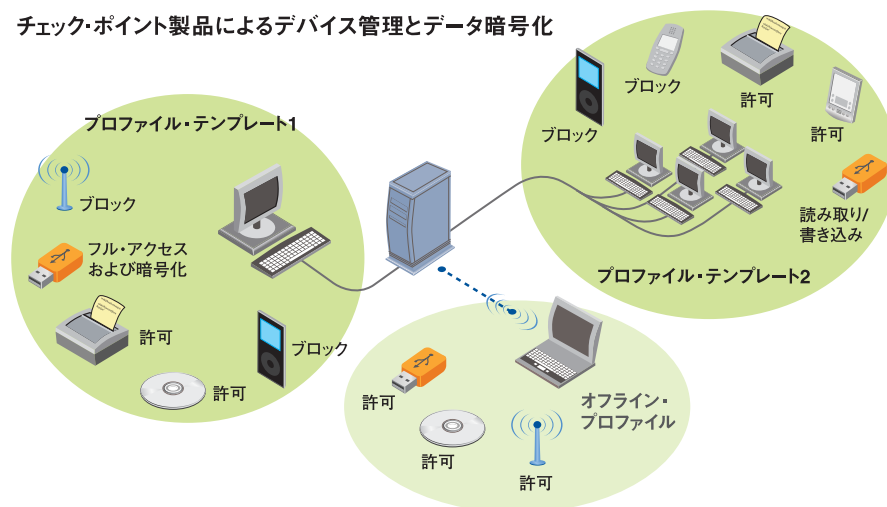
## PCI要件3.4.1の監査ガイドラインの遵守

Check Point Full Disk Encryptionは、ドライバ・ベースの起動前アクセス制御技術を用いることにより、暗号化されたファイル・システムへの論理的アクセスをオペレーティング・システムから完全に分離します。認証を受けなければマシンは起動しないため、権限のないユーザは、復号鍵を含め、ディスク上のデータには一切アクセスできません。チェック・ポイントの暗号化技術は、あらゆるリムーバブル・メディアも自動的に保護できます。

## 要件の確実な遵守を可能にする包括的な制御

Check Point Full Disk Encryptionは、起動前認証機能を始め、小売環境のエンドポイントに保存されたPCI関連データを保護するための包括的な制御機能を提供します。起動前認証機能は、既知のあらゆる攻撃手法からオペレーティング・システムを保護し、その保存場所やアプリケーションの種類、保存形式を問わず、エンドポイント上にあるすべてのPCI関連データを守ります。ローカルの独自データベースに対する認証が成功しない限り、復号鍵へのアクセスもネットワーク接続も許可されません。またCheck Point Media Encryptionは、ポートとストレージ・デバイスの管理機能を提供することにより、PCI関連データが許可なくデバイスにコピーされるのを防ぐと共に、許可されたデバイスにコピーするデータを暗号化できるようにします。

## チェック・ポイント製品によるデバイス管理とデータ暗号化



## 詳細について

保存されたカード会員情報の保護に関するPCI要件の詳細については、チェック・ポイントまでお問い合わせください。チェック・ポイントのデータ・セキュリティ製品は、小売環境の規模を問わず、迅速かつ自動的に、周囲への影響を最小限に抑えつつ導入することができます。集中的な管理と運用が可能であるため、大規模環境においても効率的に保存データを保護し、PCI規格を遵守できます。詳細については、チェック・ポイントまでお問い合わせいただくか、[www.checkpoint.co.jp/products/datasecurity/index.html](http://www.checkpoint.co.jp/products/datasecurity/index.html)をご覧ください。

## 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 (<http://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、変化し続けるお客様のビジネス・ニーズに応じてカスタマイズ可能なトータル・セキュリティ・ソリューション群を提供しています。統合されたゲートウェイ、単一エージェントによるエンドポイント、および単一の管理アーキテクチャで構成されるこのトータル・セキュリティ・ソリューション群は、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/エンドポイント・セキュリティ、データ・セキュリティ、およびVPN市場におけるリーダーシップと技術革新に基づく独自性を備えています。チェック・ポイントは、情報セキュリティの分野のみに注力するセキュリティの専門企業です。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を保護する、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。また、業界をリードするエンドポイント/データ・セキュリティ・ソリューションであるCheck Point Endpoint Security製品ラインナップを通じ、PCやモバイル端末に保存されてい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。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。

©2003-2008 Check Point Software Technologies Ltd. All rights reserved.

Check Point, AlertAdvisor, Application Intelligence, Check Point Endpoint Security, Check Point Endpoint Security On Demand, Check Point Express, Check Point Express Cl, Check Pointのロゴ, ClusterXL, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoreXL, 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, Pointsec, Pointsec Mobile, Pointsec PC, Pointsec Protector, Policy Lifecycle Management, Provider-1, PureAdvantage, PURE Security, puresecurityの logo, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, Security Management Portal, 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, SMP, SMP On-Demand, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, UTM-1, UTM-1 Edge, UTM-1 Edge Industrial, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express Cl, VPN-1 Power, VPN-1 Power Multi-core, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, 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、5,987,611、6,496,935、6,873,988、6,850,943、および7,165,076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。

Protecting Stored Cardholder Data for PCI Compliance

P/N:502829-J 2008.04

※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。

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

Tel: 03(5367)2500

E-mail: [info\\_jp@checkpoint.com](mailto:info_jp@checkpoint.com)

<http://www.checkpoint.co.jp/>