

PCI DSS (Payment Card Industry Data Security Standard) は、販売時 (POS)、送信中、および保管時におけるカード会員のデータや情報のセキュリティ確保を目的に策定されました。この標準は、クレジット カード情報を保存、処理、または送信するすべての企業に関係するものです。つまり、PCI 標準はほぼすべての業界に関係しています。

データの^{きたい}危殆化には高いリスクが伴うので、商業事業者が PCI セキュリティ標準に準拠していない場合は厳格な罰則が科されます。PCI 準拠の期限を守らなかった企業は、罰金、罰則、サービス手数料の負担増が科せられます。セキュリティ違反は訴訟に至ることもあり、その場合は企業のブランドに傷が付き、財務上の損失につながりかねません。

PCI 標準に準拠した企業は、責任を持って顧客データの保護に対処していることを効果的に示すことができ、その機会を活かして強固な顧客ロイヤルティを築くことができます。PCI 準拠を達成するための基準は多少広範囲に及びますが、すべての商業事業者は現在のネットワーク、ポリシー、およびプロセスを監査することを求められます。その目的は、明確に定義され、行き届いた監視が可能で、柔軟性のある PCI ソリューションを確立することです。

PCI DSS の要件	
安全性の高いネットワークの構築と維持	1. ファイアウォール構成を導入して維持する 2. システム パスワードにベンダー提供のデフォルトを使用しない
カード会員のデータ保護	3. 保存データを保護する 4. カード会員のデータや機密情報をパブリック ネットワーク 経由で送信する場合は暗号化する
脆弱性管理プログラムの維持	5. アンチウイルス ソフトウェアを定期的に更新する 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
強力なアクセス コントロール方法の実装	7. データへのアクセスを業務上の必要範囲内に制限する 8. コンピュータにアクセスする利用者ごとに一意な ID を割り当てる 9. カード会員データへの物理的アクセスを制限する
定期的なネットワークの監視とテスト	10. ネットワーク リソースとカード会員のデータに対する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 システムおよびプロセスを定期的にテストする
情報セキュリティ ポリシーの維持	12. 情報セキュリティに関するポリシーを維持する

Cisco Security Agent は 12 項目の PCI 1.1 要件のうち 9 項目に対応しています。

Cisco Security Agent はシスコ PCI ソリューションのエンドポイント セキュリティ コンポーネントです。サーバ、デスクトップ、ノート PC、および POS 端末で動作します。ワームや Day-Zero 攻撃から防御するとともに、サーバとクライアントの両方に対して情報の盗難を防ぐ高度な保護機能を提供します。

Cisco Security Agent は、PCI DSS の 12 分野の要件のうち、9 分野に対応しています。¹ Cisco Security Agent はポリシーベースのアーキテクチャを使用しているので、特定の使用許可要件を簡単に適用できます。これらの多くは製品に反映されています (データ盗難防止や音楽のダウンロード禁止など)。シスコでは、PCI の各要件に対応した一連の Cisco Security Agent ポリシーを作成しました。これらのポリシーは、Cisco Security Agent がサーバ、デスクトップ、ノート PC または POS 端末のいずれにインストールされていても使用可能です。

CSA ポリシーがカバーする PCI 要件	
• 1.3.5	• 7.x (拒否、読み取り、読み取り/書き込み)
• 1.3.9 (内部システム)	• 10.2.1 ~ 10.2.4 (コンプライアンス)
• 1.3.9 (外部システム)	• 10.2.1 ~ 10.2.4 (管理者追跡)
• 2.1.1	• 10.5.1 ~ 10.5.2 (ユーザ状態)
• 2.2.2	• 10.5.1 ~ 10.5.5 (コンプライアンス)
• 3	• 11.4
• 5.1.1	• 11.5
• 5.2	• 12.3.10
• 6.0	• 12.5.5 (拒否、読み取り、読み取り/書き込み)
• 6.5	

Cisco Security Agent の PCI ポリシーには以下が含まれます。

- 26 個の Cisco Security Agent ポリシー モジュール
- 150 項目の Cisco Security Agent ルール
- 9 カテゴリ、32 項目の詳細な PCI 要件の記述
- ポリシーおよびルールの記述に関連する PCI 要件の参考資料
- PCI 対象範囲に含まれるエージェントのグループに PCI ポリシーを関連付けるグループ化機能
- アプリケーションごとのサービス品質 (QoS) の優先順位付けなど、他の Cisco Security Agent ポリシーと組み合わせて使用できる機能

¹ シスコの小売店舗参照アーキテクチャの一部として CyberTrust 社の PCI 監査により検証済み。
http://www.cisco.com/web/strategy/retail/pci_imp.html

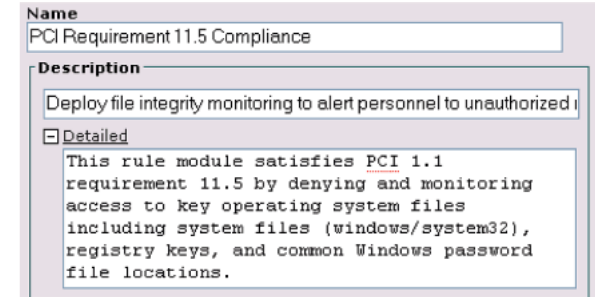
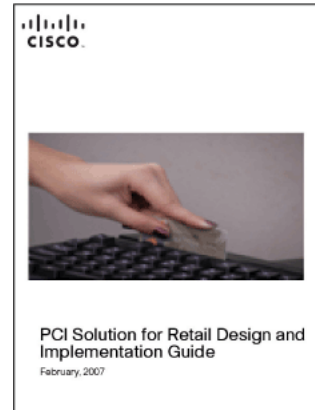
Cisco Security Agent ポリシーには、要件の意図が監査担当者にわかりやすく取り入れてあるので、監査が容易になります。特定の要件がポリシー名に反映されており、ポリシーの機能を明示的に呼び出すことができます。監査担当者が Cisco Security Agent に不慣れな場合でも、どの PCI 要件が対象になっているのか、Cisco Security Agent がどのように対象要件に対応しているのか、どのシステムに PCI ポリシーが適用されているのかを簡単に理解できます。Cisco Security Agent のロールベース アクセス コントロール機能により、監査担当者は Cisco Security Agent Management Center に読み取り専用で直接アクセスし、設定を変更することなく監査を実行できます。



Management Center for Cisco Security Agents V5.2		
Events Systems Configuration Analysis Maintenance Reports Search Help		
Compliance		is necessary for the cardholder data environment.
<input type="checkbox"/> PCI Requirement 1.3.9 Compliance - External Systems	4 rules	Installation of personal firewall software required on any mobile or employee-owned computers with direct Internet connectivity.
<input type="checkbox"/> PCI Requirement 1.3.9 Compliance - Internal Systems	5 rules	Installation of personal firewall software required on any mobile or employee-owned computers with direct Internet connectivity.
<input type="checkbox"/> PCI Requirement 10.2.1 - 10.2.4 Compliance	2 rules	Track and monitor all access to network resources and cardholder data.
<input type="checkbox"/> PCI Requirement 10.2.1 - 10.2.4 Compliance Userstate Admin	1 rule	Track and monitor all access to network resources and cardholder data (especially those with administrative privileges).
<input type="checkbox"/> PCI Requirement 10.5.1-10.5.2 User State	1 rule	Limit viewing of audit trails to those with a job-related need. Protect audit trail files from unauthorized modifications.
<input type="checkbox"/> PCI Requirement 10.5.1-10.5.5 Compliance	3 rules	Limit viewing of audit trails to those with a job-related need. Protect audit trail files from unauthorized modifications.
<input type="checkbox"/> PCI Requirement 11.4 Compliance	7 rules	Network intrusion detection systems, host-based intrusion detection systems/intrusion prevention systems to monitor networks.

また、Cisco Security Agent はシスコの自己防衛型ネットワークのコア コンポーネントとして、エンドポイント セキュリティとネットワーク セキュリティを次のように連携させます。

- IPS とファイアウォールのコラボレーションにより脅威の検出と抑制を強化
- エンドポイントに NAC (ネットワーク アドミッション コントロール) を適用することでセキュリティ保証を強化
- アプリケーションごとの QoS 優先順位付けによって POS アプリケーションのアプリケーションの優先度を強化



シスコの監査機能付き PCI 準拠アーキテクチャの包括的な設計と実装ガイドなど、Cisco Security Agent を使用した PCI 準拠の詳細については、<http://www.cisco.com/go/retail> (英語) を参照してください。データ盗難防止のデモンストレーション ビデオなど、Cisco Security Agent の詳細については、<http://www.cisco.com/jp/go/csa/> を参照してください。

© 2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。

本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(0805R)

この資料に記載された仕様は予告なく変更する場合があります。