



# PCIDSS とシスコ製品のマッピング

2009年2月25日  
シスコシステムズ

## PCI DSS version 1.2 要件とシスコ製品のマッピング

【要件1】 カード会員データを保護するためにファイアウォールを導入し、最適な設定を維持すること	
Cisco Router (IOS Firewall feature)	特にイントラネット境界などに最適 (v1.2で追記)
Cisco Catalyst 6500 with Firewall Service Module (FWSM)	LAN Switch 統合型 仮想化対応ファイアウォール
Cisco ASA5500	仮想化対応 ファイアウォール/UTM
Cisco Aironet/Wireless LAN Controller	無線ネットワーク境界の制御、保護
Cisco Security Agent	ホストベースのファイアウォール
Cisco Security MARS	ログのリアルタイム分析と設定への反映
Cisco Security Manager	統合セキュリティ管理による迅速なポリシー反映
Cisco Works Network Compliance Manager (NCM)	機器設定の管理、監査、ルータ設定ファイルの安全性と正確性の確保
Cisco Wireless Control Systems (WCS)	無線LAN機器設定の管理、監査

## PCI DSS version 1.2 要件とシスコ製品のマッピング

【要件2】 システムパスワードと他のセキュリティ・パラメータにベンダー提供のデフォルトを使用しないこと	
Cisco製ネットワークデバイスなど	SNMPなど、デフォルトパラメータ以外の設定
Cisco Secure ACS	ネットワーク機器のログイン認証
Cisco Security Agent	エンドポイントのセキュリティハードニング
Cisco Security MARS	デフォルトパラメータを使用する不正ログインの監視
Cisco Security Manager	統合セキュリティ管理による漏れのないポリシー設定
CiscoWorks Network Compliance Manager (NCM)	機器設定の管理、監査
Cisco Aironet/Wireless LAN Controller / WCS	認証、暗号伝送のための強力な暗号技術の有効化、無線LAN機器のデフォルト設定の検知、警告

【要件3】 保存されたカード会員データを安全に保護すること	
Cisco Security Agent	エンドポイントのふるまい検知/データ識別により情報漏えいを防止
Cisco Security MARS	エンドポイントログのリアルタイム分析と通知
Cisco MDS 9000 (Storage Media Encryption)	ストレージメディアの暗号化

## PCI DSS version 1.2 要件とシスコ製品のマッピング

【要件4】 公衆ネットワーク上でカード会員データを送信する場合、暗号化すること	
Cisco Router	IPsec/SSL VPN (サイト間VPN/中小規模リモートアクセス)
Cisco Catalyst 6500 with VPN SPA module	IPsec VPN (サイト間VPN / 中小規模リモートアクセス)
Cisco ASA5500	IPsec/SSL VPN (サイト間VPN/中小規模リモートアクセス)
Cisco Aironet/Wireless LAN Controller/WCS	WPA2による無線LAN暗号化/WEPの利用禁止
Cisco Ironport C-Series	メール暗号化
Cisco Security Agent	暗号化されていない無線LANネットワーク利用の禁止
Cisco Security MARS	VPN/Wireless LAN上関連のログのリアルタイム分析
Cisco Security Manager	VPN統合設定／管理
CiscoWorks Network Compliance Manager (NCM)	機器設定の管理、監査
Cisco Aironet/Wireless LAN Controller/WCS	認証、暗号伝送のための強力な暗号技術(802.11i対応)の有効化、無線LAN機器のデフォルト設定の検知、警告
【要件5】 アンチウイルス・ソフトウェアまたはプログラムを利用し、定期的に更新すること	
Cisco Security Agent	ふるまい検知、定義ファイルベースのアンチウイルス
Cisco NAC Appliance	検疫／隔離／定義ファイルの更新
Cisco ASA5500 with CSC-SSM	ゲートウェイ型アンチウイルス
Cisco Ironport C-Series /Cisco Virus & Spam Blocker	メールゲートウェイ型アンチウイルス
Cisco Ironport S-Series	Webフィルタリング型アンチマルウェア
Cisco Security MARS	エンドポイントログのリアルタイム分析と通知

## PCI DSS version 1.2 要件とシスコ製品のマッピング

【要件6】 安全性の高いシステムとアプリケーションを開発し、保守すること	
Cisco ACE Web Application Firewall	WAFによるWebアプリケーション攻撃の防御
Cisco Security Agent	ふるまい検知によるホストアプリケーション動作の保護
Cisco Security MARS	エンドポイントログのリアルタイム分析と通知

【要件7】 カード会員データへのアクセスを業務上の必要範囲内に制限すること	
Cisco Router (IOS Firewall feature)	アプリケーションインスペクションファイアウォール
Cisco Catalyst 6500 with Firewall Service Module	仮想化対応ファイアウォール/カットスループロキシによるアクセスに対するユーザ認証
Cisco ASA5500	仮想化対応ファイアウォール/UTM/カットスループロキシによるアクセスに対するユーザ認証
Cisco Aironet/Wireless LAN Controller/WCS	無線LAN制御/ユーザ認証/VLAN接続制御など
Cisco Security Agent	エンドポイント内でのカード会員データへのアクセス制御
Cisco Secure ACS	ユーザIDの管理と認証
Cisco Security MARS	不正アクセスログのリアルタイム分析と通知
Cisco Security Manager	統合セキュリティ管理による漏れのない設定
CiscoWorks Network Compliance Manager (NCM)	機器のアクセス制限設定の管理/監査/レポート作成

## PCI DSS version 1.2 要件とシスコ製品のマッピング

【要件8】 コンピュータにアクセスする利用者毎に個別のIDを割り当てること	
Cisco製ネットワークデバイスなど	IDによるユーザアクセスの許可
Cisco Secure ACS	ユーザIDの管理と認証
Cisco Security MARS	不正アクセスログのリアルタイム分析と通知
Cisco NAC Guest Server	ゲストアクセスユーザのID発行／管理

【要件9】 カード会員データへの物理的アクセスを制限すること	
IP Video surveillance	映像による入退室監視（日本未発売）

【要件10】 ネットワーク資源およびカード会員データに対する全てのアクセスを追跡し、監視すること	
Cisco製ネットワークデバイスなど	アクセスログの生成
Cisco ASA5500 (ASA5580)	高速外部ロギング対応 ファイアウォール
Cisco IPS4200	不正アクセス、トラフィックの監視、検知、記録
Cisco Security Agent	エンドポイント内のカード情報へのアクセス記録
Cisco Secure ACS	ユーザID認証ログの記録
Cisco Security MARS	不正アクセスログのリアルタイム分析、通知、記録、追跡
CiscoWorks Network Compliance Manager (NCM)	機器へのアクセス履歴の記録、監査
Cisco Wireless Control Systems	無線LAN機器設定の管理、監査

## PCI DSS version 1.2 要件とシスコ製品のマッピング

【要件11】 セキュリティ・システムおよび管理手順を定期的にテストすること	
Cisco製ネットワークデバイスなど	管理対象
Cisco Aironet/Wireless LAN Controller/WCS	無線専用IPSによる不正アクセスポイント、無線デバイスの検出
Cisco IPS4200	侵入検知／防止システムによるセキュリティ侵害の監視、検知、警告
Cisco Security Agent	エンドポイント内のセキュリティ侵害の監視、検知、警告
Cisco Security Manager	機器設定のワークフローによる管理
Cisco Security MARS	不正アクセスログのリアルタイム分析、通知、記録、追跡
CiscoWorks Network Compliance Manager (NCM)	機器へのアクセス履歴の記録、監査

## PCI DSS version 1.2 要件とシスコ製品のマッピング

【要件12】情報セキュリティに関するポリシーを整備すること	
Cisco ASA5500	リモートアクセス接続セッションの制御
Cisco Secure Desktop	リモートアクセス利用時のカード会員データのローカルハードドライブまたは他の外部媒体への保存の禁止
Cisco Security Agent	PC利用のポリシー策定と適用、警告メッセージによる教育
Cisco Security Manager	ポリシーの適用、PDCAサイクル運用の支援
Cisco Security MARS	ポリシーの監視、リスク分析、PDCAサイクルの運用支援
Cisco Wireless Control Systems (WCS)	無線LAN機器に関するPDCAサイクルの運用支援
CiscoWorks Network Compliance Manager (NCM)	ネットワーク機器の管理ポリシーの運用支援、レポート作成
WebEx	従業員教育、訓練の実施支援
Cisco Digital Media System (Digital signage)	従業員教育、訓練の実施支援

