PCI Data Security Standard (PCI DSS) 3.0

Req	PCI DSSアップデート	目的 / 対処した要求
1	カード会員データの流れを示すネットワーク図を最新に維持する。	文書化されたカード会員データフローは、ネットワーク図の重要な要素であることを明確にするため。
2	PCI DSSのスコープ内のシステムコンポーネントのインベントリを維持する。	効果的なスコーピング手法をサポートするため。
5	マルウェアの影響を一般には受けないシステムに対して、進化するマルウェアの脅威を評価する。	マルウェアからシステムを保護するための継続的な啓発や評価を促進するため。
6	安全なコーディング手法に含めるために、OWASP, NIST, SANS, 等に一致した一般的な脆弱性のリストを更新する。	新しい脅威に対応し、脆弱性のリストを最新に維持するため。
8	物理的なセキュリティトークン、スマートカード、証明書などの認証メカニズムについてのセキュリティ上の注	パスワード以外の認証方法を安全にするための要件を含めるべきであるというフィードバックに対応するた
9	POS端末やデバイスをタンパリング（物理的な改ざん）や（不正な）置き換えから守る。	支払い端末の物理的セキュリティに対応するため。
11	ペネトレーションテストの方法論を実装し、セグメンテーションが運用可能で効果的であることを確認するペネトレーションテストを行う。	ペネトレーションテストをより詳細にし、スコーピングの検証をより厳格にする要求に対応するため。
12	PCI DSSの要件が、サービスプロバイダ、事業体のどちらに管理されるかについて、情報を維持する。 サービスプロバイダは、該当のPCI DSS要件を維持するための責任を認める。	サードパーティセキュリティアシュアランスSIGからのフィードバックに対応するため。
General	PANが存在しない場合でも、センシティブ認証データは承認後に保存されてはならないことを明確にする。	センシティブ認証データの保護について確実な理解のため。
General	セキュリティを現状の活動に実装するためのガイダンス、および進行中のPCI DSS準拠を維持するためのベストプラクティスを追加。	PCI DSSに準拠したがその状態を維持していなかった組織のセキュリティ侵害に対応するため。 推奨事項は、準拠ではなくセキュリティに注力し、PCI DSSを日常的な習慣にする、カード会員データを保護するための積極的なアプローチを組織がとることを支援することに注力している。
General	以前の「PCI DSSナビゲート」から、すべての要件についてガイダンスを追加。	セキュリティ対策方針と各要件の意図の理解を支援するため。
General	ROCレポーティングセクションをレポートのテンプレートから分割。	報告プロセスを簡素化し、合理化するため。
General	各要件に期待される検証のレベルを明確にするためテスト手順を追加。	アセスメントの品質と一貫性を強調するため。
Multiple	（旧12.1.1および12.2に代えて）各要件にセキュリティポリシー/手順の要件を組み込む。	ポリシーのトピックは、関連する技術的なPCI DSSの要件に、より密に合わせる必要があるというフィードバックに対応するため。
2	デフォルトパスワードの変更はユーザアカウントと同様にアプリケーションやサービスアカウントにも必要であることを明確化。	セキュリティ侵害につながる基本的なパスワードセキュリティの習慣のギャップに対応するため。
3	暗号鍵の安全な保管に、より多くのオプションによる柔軟性を提供し、鍵の知識分割と二重管理の原則について明確化。	鍵管理についての一般的な誤解を明確化するため。
8	パスワードの長さと複雑さについて同等のバリエーションを認め、柔軟性を向上。 強力なパスワードの選択、認証情報の保護、および漏洩が疑われるパスワードの変更についてのユーザ向けガイダンスを含むパスワードポリシーの改訂。	パスワードセキュリティの改善についてのフィードバックに対応するため。新しい要件ではなく、柔軟性の向上とユーザへのガイダンスに注力した変更。
10	日次ログレビューの目的と範囲の明確化。	事業体が不審な活動の識別に効果的なログレビューに注力し、事業体のリスク管理戦略によって定義される重要度の低いログやイベントのレビューについて柔軟性を認めることを支援するため。

「PCI DSS and PA-DSS – Version 3.0 Change Highlights August 2013 （Copyright 2013 PCI Security Standards Council LLC）」より引用

※本翻訳は当社非公式訳となります。翻訳内容についてPCISSCへのお問い合わせはご遠慮ください。
お問い合わせは、NTTデータ先端技術株式会社「E-mail：pci@intellilink.co.jp, TEL:03-5859-5428」までお願い致します