本翻訳文書について
本翻訳文書は、NTTデータ先端技術株式会社によるサービスとして情報提供されます。これは、
「https://www.pcisecuritystandards.org/security_standards/documents.php copyright © 2006-2015 PCI セキュリティスタンダーズカウンシル LLC」で公開されるオフィシャルドキュメントである「Summary of Changes from PCI DSS Version 3.0 to 3.1」の、非公式の翻訳です。
英文が、本ドキュメントのオフィシャルバージョンであるとみなされ、翻訳文と英文においての曖昧さや不明瞭さについては、英文が優先されます。翻訳版は、PCI SSC と NTTデータ先端技術株式会社間における翻訳許諾契約で明記される条件のもと、公開されます。PCI セキュリティスタンダーズカウンシル LLC も NTTデータ先端技術株式会社も、本翻訳文書に含まれる過失に対する責任を負いません。

About this translation:
"This translated document is provided by NTT DATA INTELLILINK CORPORATION as an informational service. This is an unofficial translation of the official document, Summary of Changes from PCI DSS Version 3.0 to 3.1 located at https://www.pcisecuritystandards.org/security_standards/documents.php copyright © 2006-2015 PCI Security Standards Council LLC. The English text to be found at such address shall for all purposes be regarded as the official version of this document, and to the extent of any ambiguities or inconsistencies between this text and the English text, the English text at such location shall control. This translation is published with acknowledgement of and in agreement with terms specified in a translation permissions agreement between PCISSC and NTT DATA INTELLILINK CORPORATION. Neither PCI Security Standards Council LLC nor NTT DATA INTELLILINK CORPORATION assume responsibility for any errors contained herein."

【注意事項】
- 本文書は、NTTデータ先端技術株式会社が翻訳を行い、独自に公開するものです。
- 本文書では、”Table 2: Summary of Changes”のみを翻訳対象としています。
- 本文書の内容について、PCI SSC へのお問い合わせはご遠慮ください。お問い合わせは、以下の連絡先までお願いいたします。
  NTTデータ先端技術株式会社 E-mail: pci@intellilink.co.jp TEL: 03-5859-5428

表2：変更点のまとめ

Section		Change	変更点（翻訳）	種類
PCI DSS v3.0	PCI DSS v3.1			
All	All	Addressed minor typographical errors (grammar, punctuation, formatting, etc.) and incorporated minor updates for readability throughout the document.	いくつかの誤植に対処し（文法、句読点、書式設定など）、文書全体の可読性を向上するためにいくつかの更新を行った。	明確化（Clarification）
Introduction	Introduction	Changed reference from “protecting cardholder data” to “protecting account data”.	「カード会員データを保護する」から「アカウントデータの保護」に基準を変更した。	明確化（Clarification）
Introduction	Introduction	Clarified that PCI DSS applies to any entity that stores, processes or transmits account data.	PCI DSSはアカウントデータを保存、処理、または伝送するいかなる企業にも適用されることを明確にした。	明確化（Clarification）
Introduction	Introduction	Changed reference from “personally identifiable information” to “personal information”.	「個人を識別可能な情報」から「個人情報」に表現を変更した。	明確化（Clarification）
PCI DSS Applicability	PCI DSS Applicability	Changed reference from “financial institutions” to “acquirers, issuers”.	「金融機関」から「アクワイアラ、イシュア」に表現を変更した。	明確化（Clarification）
PCI DSS Applicability Information	PCI DSS Applicability Information	Removed reference to “environments” to clarify applicability at the organization level rather than the system level.	システムレベルではなく組織レベルへの適用性を明確にするため「環境」の表現を削除した。	明確化（Clarification）
Scope of PCI DSS Requirements	Scope of PCI DSS Requirements	Aligned with language used earlier in the same section regarding steps for confirming accuracy of the defined CDE.	CDE定義の精度を確認するための手順について、前のバージョンの同じセクションで使用する文言を合わせた。	明確化（Clarification）
Use of Third Party Service Providers / Outsourcing	Use of Third Party Service Providers / Outsourcing	Clarified that validation processes for service providers include undergoing their own annual assessments or undergoing multiple on-demand assessments.	サービスプロバイダーのための検証プロセスに独自の年次評価を実施していること、または外部の審査を受けていることが含まれるように明確にした。	明確化（Clarification）
PCI DSS Assessment Process	PCI DSS Assessment Process	Reordered assessment steps to clarify that a ROC, SAQ, or AOC may be submitted without all requirements being “in place”.	ROC、SAQ、またはAOCはすべての要件が“適合”でなくとも提出ができることを明確にするため、評価の手順を見直した。	明確化（Clarification）
General	General	Updated language in requirements and/or testing procedures for consistency.	要件および/またはテスト手順について一貫性のある文言に更新した。	明確化（Clarification）
2.2.3	2.2.3	Removed SSL as an example of a secure technology. Added note that SSL and early TLS are no longer considered to be strong cryptography and cannot be used as a security control after June 30, 2016. Additional guidance provided in Guidance column. Also impacts Requirements 2.3 and 4.1.	安全な技術の一例としてSSLを削除した。SSLと初期のTLSはもはや強力な暗号化であるとみなされず、2016年6月30日後にセキュリティコントロールとして使用することができないことを注記に追加した。追加のガイダンスをガイダンス列に追記した。要件2.3と4.1にも同様の影響がある。	発展型要件（Evolving Requirement）

© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.

Section		Change	変更点（翻訳）	種類
PCI DSS v3.0	PCI DSS v3.1			
2.3	2.3	Removed SSL as an example of a secure technology and added a note to the requirement. See explanation above at 2.2.3.	安全な技術の一例としてSSLを削除し、要件に注記を追加した。 前述の2.2.3での説明を参照。	発展型要件（Evolving Requirement）
3.2.1 – 3.2.3	3.2.1 – 3.2.3	Clarified in requirements that storage of sensitive authentication data is not permitted “after authorization”.	“承認後”の機密認証データの保存について許可されない要件を明確にした。	明確化（Clarification）
3.4	3.4	Clarified in requirement note that additional controls are required if hashed and truncated versions of the same PAN are present in an environment. Added Testing Procedure 3.4.e to assist with validation of the Note. Clarified intent of “truncation” in Guidance Column.	同じPANのハッシュ化したものとトランケートしたものが環境に存在する場合は、追加のコントロールが必要であることを要件の注記内で明確にした。注記の検証を支援するテスト手順3.4.eを追加した。ガイダンス列に“トランケーション”の目的を明確にした。	明確化（Clarification）
3.5.2	3.5.2	Clarified that “HSM” may refer to a “Hardware” or “Host” Security Module. Aligned with language in PCI PTS.	「HSM」は「ハードウェア」または「ホスト」セキュリティモジュールを指すことを明確にした。PCI PTSにおける文言と整合性を保った。	明確化（Clarification）
3.6	3.6	Clarified that Testing Procedure 3.6.a only applies if the entity being assessed is a service provider.	テスト手順3.6.aが適用されるのは評価対象の事業体がサービスプロバイダの場合のみであることを明確にした。	明確化（Clarification）
4.1	4.1	Removed SSL as an example of a secure technology and added a note to the requirement. See explanation above at 2.2.3.	安全な技術の一例としてSSLを削除し、要件に注記を追加した。前述の2.2.3での説明を参照。	発展型要件（Evolving Requirement）
4.1.1	4.1.1	Updated testing procedure to recognize all versions of SSL as examples of weak encryption.	弱い暗号化の例としてSSLのすべてのバージョンを認識するテスト手順に更新した。	発展型要件（Evolving Requirement）
4.2	4.2	Included SMS as an example of end-user messaging technology and added guidance.	エンドユーザメッセージングテクノロジの例としてSMSを含めるようにし、ガイダンスを追加した。	明確化（Clarification） 追加のガイダンス（Additional Guidance）
6.6	6.6	Added clarification to testing procedure and Guidance column that if an automated technical solution is configured to alert (rather than block) web-based attacks, there must also be a process to ensure timely response.	自動化された技術的な解決策がWebベースの攻撃に対して（ブロックではなく）警告を挙げるよう構成されている場合、タイムリーな応答を確保するためのプロセスが存在しなければならないようテスト手順とガイダンスの明確化を行った。	明確化（Clarification）
8.1.4	8.1.4	Clarified that inactive user accounts must be removed/disabled within 90 days.	非アクティブなユーザーアカウントが90日以内に削除/無効にしなければならないことを明確にした。	明確化（Clarification）
8.1.6.b 8.2.1.d 8.2.1.e 8.2.3.b 8.2.4.b 8.2.5.b	8.1.6.b 8.2.1.d 8.2.1.e 8.2.3.b 8.2.4.b 8.2.5.b	Clarified that Testing Procedure only applies if the entity being assessed is a service provider, and for non-consumer customer accounts.	評価されている事業体がサービスプロバイダで、非消費者の顧客アカウントに対してのみ、テスト手順が適用されることを明確にした。	明確化（Clarification）
8.2.4	8.2.4	Clarified that passwords must be changed at least once every 90 days.	パスワードは90日ごとに少なくとも一度変更する必要があることを明確にした。	明確化（Clarification）
8.5.1	8.5.1	Clarified this requirement only applies if the entity being assessed is a service provider.	この要件が適用されるのは評価対象の事業体がサービスプロバイダの場合のみであることを明確にした。	明確化（Clarification）
9.2	9.2	Clarified that the requirement applies to all onsite personnel and visitors. Combined Testing Procedures 9.2.b and 9.2.d to remove redundancy.	すべてのオンサイト担当者と訪問者に対して要件が適用されることを明確にした。 冗長な記載を削除するためテスト手順9.2.bと9.2.dを統合した。	明確化（Clarification）
9.9.1.b	9.9.1.b	Updated testing procedure to clarify both devices and device locations need to be observed.	デバイスとデバイスの場所両方が観察されなければならないことを明確にするため、テスト手順を更新した。	明確化（Clarification）
10.6	10.6	Removed redundant language in guidance column.	ガイダンス列の冗長な文言を削除した。	明確化（Clarification）
10.6.1	10.6.1	Updated requirement to more clearly differentiate intent from Requirement 10.6.2.	より明確に要件10.6.2と意図を区別するため、要件を更新した。	明確化（Clarification）
11.1.c	11.1.c	Clarified that testing procedure applies where wireless scanning is utilized.	無線スキャンを利用する場合に適用されるテスト手順を明確にした。	明確化（Clarification）

© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.

Section		Change	変更点（翻訳）	種類
PCI DSS v3.0	PCI DSS v3.1			
11.2	11.2	Clarified in Guidance Column that a vulnerability scan could be a combination of automated and manual tools, techniques, or other methods.	脆弱性スキャンは、自動と手動のツール、技術、または他の方法の組み合わせであることをガイダンス列で明確にした。	追加のガイダンス（Additional Guidance）
11.3.2.a	11.3.2.a	Removed redundant language from testing procedure.	テスト手順の冗長な言葉を削除した。	明確化（Clarification）
11.3.4	11.3.4	Clarified that the intent of the penetration testing is to verify that all out-of-scope systems are segmented (isolated) from systems “in the CDE”.	ペネトレーションテストは、全てのスコープ外システムがCDE内のシステムから分割（分離）されていることを検証する意図であることを明確にした。	明確化（Clarification）
11.5	11.5	Clarified that unauthorized modifications include changes, additions, and deletions of critical system files, etc.	不正な変更には、緊急性の高いシステムファイル等への変更、追加、および削除が含まれることを明確にした。	明確化（Clarification）
12.2	12.2	Clarified that the risk assessment process must result in a formal, “documented analysis of risk”.	リスク評価のプロセスが、正式な“文書化されたリスク分析”の結果に至る必要があることを明確にした。	明確化（Clarification）
12.9	12.9	Clarified this requirement only applies if the entity being assessed is a service provider and added related guidance.	この要件が適用されるのは、評価対象の事業体がサービスプロバイダの場合のみであることを明確にし、関連するガイダンスを追加した。	明確化（Clarification） 追加のガイダンス（Additional Guidance）
Appendix C: Compensating Controls Worksheet – Completed Example	Appendix C: Compensating Controls Worksheet – Completed Example	Updated description of compensating control example to reflect use of “sudo” rather than “SU” for improved technical accuracy.	技術的正確さを改善するため、“su”ではなく、“sudo”を使用するよう、代替コントロール例の説明を更新した。	追加のガイダンス（Additional Guidance）

© 2006-2015 PCI Security Standards Council, LLC. All Rights Reserved.