表2：変更点のまとめ

Section		Change	変更点（翻訳）	種類
PCI DSS v3.1	PCI DSS v3.2			
All	All	Addressed minor typographical errors (grammar, punctuation, formatting, etc.) and incorporated minor updates for readability throughout the document.	誤植の修正（文法、句読点、書式設定など）、および全体の可読性を向上させる更新を行った。	明確化 (Clarification)
Relationship between PCI DSS and PA-DSS	Relationship between PCI DSS and PA-DSS	Added guidance that security threats are constantly evolving, and payment applications that are not supported by the vendor may not offer the same level of security as supported version.	セキュリテイに対する脅威が常に進化している事、およびベンダサポートが終了しており、サポートされているバージョンと同レベルのセキュリティが提供されないペイメントアプリケーションに関するガイダンスを追加した。	追加のガイダンス (Additional guidance)
Scope of PCI DSS Requirements	Scope of PCI DSS Requirements	Clarified that backup/recovery sites need to be considered when confirming PCI DSS scope.	PCI DSS対象範囲を判断する際、バックアップ/リカバリサイトを考慮する必要があることを明確化した。	明確化 (Clarification)
Best Practices for Implementing PCI DSS into Business-as-Usual Processes	Best Practices for Implementing PCI DSS into Business-as-Usual Processes	Updated Note to clarify that some business-as-usual principles may be requirements for certain entities, such as those defined in the Designated Entities Supplemental Validation (Appendix A3).	注記を更新して、DESV（付録 A3）で定義されている、いくつかの日常業務に関する原則が特定の事業体に対する要件となる場合がある事を明確化した。 DESV：指定事業体に対する補足検証事項	明確化 (Clarification)
	PCI DSS Versions	New section to describe how this version of PCI DSS impacts the previously-effective version.	このバージョンが、一つ前の有効なバージョンに対してどのような影響を与えるかについて記述するセクションを追加した。	追加のガイダンス (Additional guidance)
要件(Requirements)				
General	General	Removed examples of “strong” or “secure” protocols from a number of requirements, as these may change at any time.	いくつかの要件から、"強力な"または"安全な"プロトコルの例を削除した。どのようなプロトコルを"強力"または"安全"と見なせるかは、いつでも変わり得るためである。	明確化 (Clarification)
General	General	Moved examples from a number of requirements and/or testing procedures to the Guidance column, and added guidance where appropriate.	いくつかの要件および/またはテスト手順に記載していた例をガイダンス列に移動し、必要に応じてガイダンスを追加した。	明確化 (Clarification)
General	General	Changed “passwords/phrases” to “passwords/passphrases” in a number of requirements for consistency.	表記の整合性を保つため、いくつかの要件における"passwords/phrases"を"passwords/passphrases"に変更した。	明確化 (Clarification)
General	General	Clarified correct term is multi-factor authentication, rather than two-factor authentication, as two or more factors may be used.	2つ以上の要素が使用され得るため、二要素認証ではなく、多要素認証を正しい用語として明確化した。	明確化 (Clarification)
General	General	Removed notes from requirements referring to an effective date of July 1, 2015, as these are now effective. Affected requirements are 6.5.10, 8.5.1, 9.9, 11.3, and 12.9.	発効日が2015年7月1日である要件について、既に有効となったため、注記を削除した。影響のある要件は6.5.10, 8.5.1, 9.9, 11.3, および12.9である。	明確化 (Clarification)
1.1.6	1.1.6	Clarified that approval of business use is included in the justification. Removed examples of “insecure” protocols as these may change in accordance with industry standards.	業務上の正当性に、業務利用の承認が含まれるよう明確化した。 "安全でない"プロトコルの例を削除した。これらは、業界標準に従って変わっていくためである。	明確化 (Clarification)
1.2.1	1.2.1	Added guidance to clarify intent of requirement.	要件の意図を明確にするためにガイダンスを追加した。	明確化 (Clarification)
1.3	1.3	Added guidance to clarify intent of requirement.	要件の意図を明確にするためにガイダンスを追加した。	明確化 (Clarification)
1.3.3		Removed requirement as intent is addressed via other requirements in 1.2 and 1.3.	1.2および1.3の中の他の要件を通じて対処されるため、本要件を削除した。	明確化 (Clarification)

Section		Change	変更点（翻訳）	種類
PCI DSS v3.1	PCI DSS v3.2			
1.3.4 – 1.3.8	1.3.3 – 1.3.7	Renumbered due to removal of former Requirement 1.3.3.	直前の要件1.3.3を削除したため、採番し直した。	明確化 (Clarification)
1.3.6	1.3.5	Updated to clarify intent of requirement rather than use of a particular type of technology.	要件の意図するところが、特定の種類の技術の使用ではないことを明確化した。	明確化 (Clarification)
1.4	1.4	Increased flexibility by including or equivalent functionality as alternative to personal firewall software. Clarified requirement applies to all portable computing devices that connect to the Internet when outside the network and that also access the CDE.	パーソナルファイアウォールだけでなく、同等の機能を持つ代替手段も含めることで、要件を柔軟にした。 外部ネットワーク接続時にインターネットに接続し、CDEにもアクセスする全てのポータブルデバイスに要件を適用することを明確化した。	明確化 (Clarification)
2.1	2.1	Clarified requirement applies to payment applications.	ペイメントアプリケーションに要件が適用されることを明確化した。	明確化 (Clarification)
2.2.3	2.2.3	Removed note and testing procedures regarding removal of SSL/early TLS and moved to new Appendix A2.	SSL/初期のTLSの廃止に関する注記とテスト手順を削除して、新しい付録 A2 へ移動した。	明確化 (Clarification)
2.3	2.3	Removed note and testing procedures regarding removal of SSL/early TLS and moved to new Appendix A2. Removed reference to “web-based management” as requirement already specifies “all non-console administrative access”, which by definition includes any web-based access.	SSL/初期のTLSの廃止に関する注記とテスト手順を削除して、新しい付録 A2 へ移動した。 "Webベース管理"に関する言及を削除した。これは、要件で既に"非コンソール管理アクセス"が指定されており、また定義により任意のWebベースアクセスは"非コンソール管理アクセス"に含まれるためである。	明確化 (Clarification)
3.3	3.3	Updated requirement to clarify that any displays of PAN greater than the first six/last four digits of the PAN requires a legitimate business need. Added guidance on common masking scenarios.	先頭6文字/末尾4文字を超えるPANの表示について、正当な業務上の必要性が要求されることを要件で明確化した。 マスキングのよくある状況について、ガイダンスを追加した。	発展型要件 (Evolving Requirement)
3.4.d	3.4.d	Updated testing procedure to clarify the examination of audit logs includes payment application logs.	監査ログの調査にペイメントアプリケーションログを含めることをテスト手順で明確化した。	明確化 (Clarification)
3.4.1	3.4.1	Added note to requirement to clarify the requirement applies in addition to all other PCI DSS encryption and key management requirements.	この要件が、他の全ての暗号化と鍵管理に関する PCI DSS 要件に加えて適用される事を明確化するため、注記を追加した。	明確化 (Clarification)
	3.5.1	New requirement for service providers to maintain a documented description of the cryptographic architecture. Effective February 1, 2018	サービスプロバイダ向けに、暗号化アーキテクチャの文書記述を維持する新しい要件を追加した。 2018年2月1日から発効される。	発展型要件 (Evolving Requirement)
3.5.1 – 3.5.3	3.5.2 – 3.5.4	Renumbered due to addition of new Requirement 3.5.1.	新たな要件3.5.1の追加のために採番し直した。	明確化 (Clarification)
3.6.1.b	3.6.1.b	Updated testing procedure language to clarify testing involves observation of procedures rather than key-generation method itself, as this should not be observable. Added guidance referring to Glossary definition for "Cryptographic Key Generation"	鍵生成の方式自体を観察するのではなく、鍵生成手順の観察によってテストすることを明確化するため、テスト手順の文言を更新した。 「暗号鍵生成」の用語集での定義を参照するガイダンスを追加した。	明確化 (Clarification)
4.1	4.1	Removed note and testing procedures regarding removal of SSL/early TLS and moved to new Appendix A2.	SSL/初期のTLSの廃止に関する注記とテスト手順を削除して、新しい付録 A2 へ移動した。	明確化 (Clarification)
6.2	6.2	Added clarification to Guidance column that requirement to patch all software includes payment applications.	パッチを適用するすべてのソフトウェアの中にペイメントアプリケーションが含まれることを明確化するようガイダンス列に追記した。	明確化 (Clarification)
6.4.4	6.4.4	Updated requirement to align with testing procedure.	要件とテスト手順の整合性を合わせるよう更新した。	明確化 (Clarification)
6.4.5	6.4.5	Clarified that change control processes are not limited to patches and software modifications.	変更管理プロセスをパッチやソフトウェア変更に限らないように明確にした。	明確化 (Clarification)
	6.4.6	New requirement for change control processes to include verification of PCI DSS requirements impacted by a change. Effective February 1, 2018	変更管理プロセスに関する新しい要件を追加した。この要件では、変更による PCI DSS の各要件への影響を検証する事が要求される。 この要件は、2018年2月1日から発効される。	発展型要件 (Evolving Requirement)
6.5	6.5	Clarified that training for developers must be up to date and occur at least annually.	開発者のためのトレーニングを最新化すること、および少なくとも年次で行うことを明確にした。	明確化 (Clarification)
6.5.a – 6.5.d	6.5.a – 6.5.c	Removed Testing Procedure 6.5.b and renumbered remaining testing procedures to accommodate.	テスト手順6.5.bを削除し、これに合わせて残りのテスト手順を採番し直した。	明確化 (Clarification)

Section		Change	変更点（翻訳）	種類
PCI DSS v3.1	PCI DSS v3.2			
7.2	7.2	Updated requirement, testing procedures and Guidance column to clarify that one or more access control systems may be used.	一つ以上のアクセス制御システムが使用され得ることを明確にするため、要件、テスト手順およびガイダンス列を更新した。	明確化 (Clarification)
Requirement 8	Requirement 8	Added note to Requirement 8 introduction that the authentication requirements do not apply to accounts used by consumers (e.g. cardholders).	要件8の導入部分の注記に、認証に関する各要件は消費者(例.カード会員)が使用するアカウントには適用されない事を追加した。	明確化 (Clarification)
8.1.5	8.1.5	Clarified requirement intended for all third parties with remote access, rather than only vendors.	要件が対象とするのは、ベンダだけではなく、すべてのサードパーティのリモートアクセスであることを明確化した。	明確化 (Clarification)
8.2.3	8.2.3	Updated Guidance column to reflect changing industry standards.	業界標準の変更を反映するようガイダンス列を更新した。	明確化 (Clarification)
8.3	8.3	Clarified correct term is multi-factor authentication rather than two-factor authentication, as two or more factors may be used.	二要素認証ではなく、多要素認証として用語を修正し明確化した。2つ以上の要素が使用されるためである。	明確化 (Clarification)
8.3	8.3, 8.3.1, 8.3.2	Expanded Requirement 8.3 into sub-requirements, to require multi-factor authentication for all personnel with non-console administrative access, and all personnel with remote access to the CDE. New Requirement 8.3.2 addresses multi-factor authentication for all personnel with remote access to the CDE (incorporates former Requirement 8.3). New Requirement 8.3.1 addresses multi-factor authentication for all personnel with non-console administrative access to the CDE. Requirement 8.3.1 effective February 1, 2018	要件8.3を複数のサブ要件に展開して、多要素認証を、CDEに対して非コンソール管理アクセスを行う全ての担当者と、CDEにリモートアクセスする全ての担当者に対して要求するようにした。 新しい要件 8.3.2 は、CDE へのリモートアクセスを行う全ての担当者に対して多要素認証を要求する（これは前バージョンの要件 8.3 に相当する）。 新しい要件 8.3.1 は、非コンソール管理アクセスを行う全ての担当者に対して多要素認証を要求する。 要件8.3.1は2018年2月1日から発効される。	発展型要件 (Evolving Requirement)
9.1.1	9.1.1	Clarified that either video cameras or access controls mechanisms, or both, may be used.	ビデオカメラまたはアクセス制御メカニズムのどちらか、あるいは両方を使用するよう明確化した。	明確化 (Clarification)
9.5.1.a – 9.5.1.b	9.5.1	Combined testing procedures to clarify that assessor verifies the storage location is reviewed at least annually.	保管場所が少なくとも年次でレビューされていることを評価者が確認するよう明確化するため、テスト手順を統合した。	明確化 (Clarification)
	10.8, 10.8.1	New requirement for service providers to detect and report on failures of critical security control systems. Effective February 1, 2018	サービスプロバイダのための新規要件を追加した。この要件では、重要なセキュリティコントロールシステムの機能停止の検知、および報告が要求される。 この要件は、2018年2月1日から発効される。	発展型要件 (Evolving Requirement)
10.8	10.9	Renumbered due to addition of new Requirement 10.8.	新要件10.8の追加のために採番し直した。	明確化 (Clarification)
11.2.1	11.2.1	Clarified that all “high risk” vulnerabilities must be addressed in accordance with the entity’s vulnerability ranking (as defined in Requirement 6.1), and verified by rescans.	すべての「高リスク」脆弱性は事業体の脆弱性ランク付けに従って対応される必要があり(要件6.1で定義されたように)、再スキャンで検証済とすることを明確にした。	明確化 (Clarification)
11.3.4	11.3.4	Added Testing Procedure 11.3.4.c to confirm penetration test is performed by a qualified internal resource or qualified external third party.	テスト手順 11.3.4.c を追加した。この手順では、ペネトレーションテストが、認定された内部リソース、または認定された外部の第三者によって実施された事を確認する事が要求される。	明確化 (Clarification)
	11.3.4.1	New requirement for service providers to perform penetration testing on segmentation controls at least every six months. Effective February 1, 2018	サービスプロバイダのための新規要件を追加した。この要件では、セグメンテーション制御のペネトレーションテストを6カ月毎に実施する事が求められる。 この要件は、2018年2月1日から発効される。	発展型要件 (Evolving Requirement)
11.5.a	11.5.a	Removed “within the cardholder data environment” from testing procedure for consistency with requirement, as requirement may apply to critical systems located outside the designated CDE.	要件の一貫性を保つためにテスト手順から「カード会員データ環境内」を削除した。これは、CDEの外側に位置する重要なシステムにもこの要件が適用される場合があるためである。	明確化 (Clarification)
12.3.3	12.3.3	Reformatted testing procedure for clarity.	テスト手順を明確にするため修正した。	明確化 (Clarification)
	12.4	New requirement for service providers’ executive management to establish responsibilities for the protection of cardholder data and a PCI DSS compliance program. Effective February 1, 2018	サービスプロバイダのための新規要件を追加した。この要件では、サービスプロバイダの経営層に対して、カード会員データの保護と PCI DSS 準拠プログラムに対する責務を確立する事が求められる。 この要件は、2018年2月1日から発効される。	発展型要件 (Evolving Requirement)
12.4	12.4.1	Renumbered due to addition of new Requirement 12.4.	新要件12.4の追加のために採番し直した。	明確化 (Clarification)
12.6	12.6	Clarified intent of security awareness program is to ensure personnel are aware of the cardholder data security policy and procedures.	セキュリティ意識向上プログラムが、カード会員データのセキュリティポリシーや手順を担当者に啓発する意図であることを明確にした。	明確化 (Clarification)

Section		Change	変更点（翻訳）	種類
PCI DSS v3.1	PCI DSS v3.2			
12.8.1	12.8.1	Clarified that the list of service providers includes a description of the service provided.	サービスプロバイダの一覧に、提供されるサービスの記述を含むよう明確にした。	明確化 (Clarification)
12.8.2	12.8.2	Added guidance that service provider responsibility will depend on the particular service being provided and the agreement between the two parties.	サービスプロバイダの責任は、提供されているサービスと両当事者間の合意事項に依存することについてガイダンスを追加した。	追加のガイダンス (Additional guidance)
12.10.2	12.10.2	Clarified that review of the incident response plan encompasses all elements listed in Requirement 12.10.1.	インシデント対応計画のレビューに要件12.10.1に記載されているすべての要素が含まれることを明確にした。	明確化 (Clarification)
	12.11, 12.11.1	New requirement for service providers to perform reviews at least quarterly, to confirm personnel are following security policies and operational procedures. Effective February 1, 2018	サービスプロバイダのための新規要件を追加した。この要件では、担当者がセキュリティポリシーと運用手順に従っている事を確認するためのレビューを、少なくとも四半期に一度、実施する事が要求される。 この要件は、2018年2月1日から発効される。	発展型要件 (Evolving Requirement)
Appendix A	Appendix A1	Renumbered Appendix “Additional PCI DSS Requirements for Shared Hosting Providers” due to inclusion of new appendices.	新たな付録を含めるために「共有ホスティングプロバイダのための追加のPCI DSS要件」付録を採番し直した。	明確化 (Clarification)
	Appendix A2	New Appendix with additional requirements for entities using SSL/early TLS, incorporating new migration deadlines for removal of SSL/early TLS.	SSL/初期のTLSを使用する事業体のための追加の要件の付録を追加した。この付録には、SSL/初期のTLSの廃止に対する新しい移行期限が含まれる。	明確化 (Clarification)
	Appendix A3	New Appendix to incorporate the “Designated Entities Supplemental Validation” (DESV), which was previously a separate document.	以前は別の文書だった「指定事業体の補足検証 (DESV)」を組み込んだ新しい付録を追加した。	明確化 (Clarification)