No.	PCI DSS要件	DBセキュリティに関する補足	DBSC ガイド	実
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インストールして構成を維持すること**	**・DBサーバーに接続できるノードは必要最小限にする。**	**4.1.6.1**	
要件：2	**システムパスワードおよび他のセキュリティパラメータにベンダ提供のデフォルト値を使用しないこと**			
2.1	システムをネットワーク上に導入する前に、ベンダ提供のデフォルト値を必ず変更する（パスワード、簡易ネットワーク管理プロトコル（SNMP）コミュニティ文字列の変更、不必要なアカウントの削除など）。	・デフォルトポートを変更する。 ・デフォルトで作成される不要なアカウントを削除または無効化する。 ・デフォルトパスワードを変更する。 ・サンプルDBを削除する。 ・パブリックなロールから不要な権限を削除する。	4.1.1.1(3) 4.1.2.1(2) 4.1.2.2(1)	★ ★ ★
2.2	すべてのシステムコンポーネントについて、構成基準を作成する。この基準は、すべての既知のセキュリティ脆弱性をカバーし、また業界で認知されたシステム強化基準と一致している必要がある。			
2.2.1	1 つのサーバには、主要機能を 1つだけ実装する。	・DBサーバでは、主としてDBMSのみを稼動させる。	-	
2.2.2	安全性の低い不必要なサービスおよびプロトコルはすべて無効にする（デバイスの特定機能を実行するのに直接必要でないサービスおよびプロトコル）。	・必要な機能を選択し、対象機能のみをインストールする。 ・使用しないDBMS機能、サービスは削除または無効化する。 ・DBサーバのOSレベルにおいても、不要な機能、サービスを削除する。 ・必要なプロトコルのみを有効にし、不要なプロトコルは無効にする。	4.1.1.1(2) 4.1.1.1(2) 4.1.6.4(1)	★ ★
2.2.3	システムの誤用を防止するためにシステムセキュリティパラメータを構成する。	・各種ベンダから提供される推奨パラメータを設定する。 例） ・データベースセキュリティガイドライン 第2.0版 http://www.db-security.org/report.html#gl02 ・DBセキュリティ 製品別機能対応表 第1.0版 http://www.db-security.org/wgimpl_seika.html		
2.2.4	スクリプト、ドライバ、機能、サブシステム、ファイルシステム、不要な Web サーバなど、不要な機能をすべて削除する。	・使用しないDBMS機能、オブジェクトなどは削除または無効化する。 ・DBサーバのOSレベルにおいても、不要な機能、サービスを削除する。	4.1.1.1(2) 4.1.6.4(1)	★
2.3	すべてのコンソール以外の管理アクセスを暗号化する。Web ベースの管理やその他のコンソール以外の管理アクセスについては、SSH、VPN、または SSL/TLS などのテクノロジを使用する。	・DBMSの暗号化通信機能を有効にする、あるいはその他の方法で通信を暗号化してDBクライアントからアクセスする。	4.1.4.1	
要件：3	**保存されたカード会員データを保護すること**			
3.4	以下の手法を使用して、すべての保存場所で PAN を少なくとも読み取り不能にする（ポータブルデジタルメディア、バックアップメディア、ログを含む）。 ・ 強力な暗号化技術をベースにしたワンウェイハッシュ ・ トランケーション ・ インデックストークンとパッド（パッドは安全に保存する必要がある） ・ 関連するキー管理プロセスおよび手順を伴う、強力な暗号化 アカウント情報のうち、少なくとも PANは読み取り不能にする必要がある。 注: ・ 何らかの理由で PAN を読み取り不能にできない場合は、「付録 B:代替コントロール」を参照。 ・ 強力な暗号化技術は、「PCI DSS Glossary of Terms, Abbreviations, and Acronyms」で定義されています。			
3.4.1	（ファイルまたは列レベルのデータベース暗号化ではなく）ディスク暗号化が使用される場合、論理アクセスはネイティブなオペレーティングシステムのアクセス制御メカニズムとは別に管理する必要がある（ローカルユーザーアカウントデータベースを使用しないなどの方法で）。暗号解除キーをユーザアカウントに結合させてはいけない。	・データ暗号化機能／ツールを利用し、格納データを暗号化する。 ・データ暗号化機能／ツールを利用し、データファイルを暗号化する。 ・データ暗号化機能／ツールを利用し、バックアップファイルを暗号化する。	4.1.4.2(1) 4.1.4.2(2) 4.1.4.2(3)	
3.5	カード会員データの暗号化に使用される暗号化キーを、漏洩と誤使用から保護する。	・適切に暗号鍵を管理する。 例） ・定期的に鍵の暗号鍵を変更する。	4.1.4.4	
3.5.1	暗号化キーへのアクセスを、必要最小限の管理者に制限する。	・暗号鍵にアクセス可能な人物を、最小限のDB管理者に限定する。	4.1.4.4	
3.5.2	暗号化キーの保存場所と形式を最小限にし、安全に保存する。	・暗号鍵を暗号化して保存する。 ・鍵の暗号鍵とデータの暗号鍵を分けて保管する。	4.1.4.4	
3.6	カード会員データの暗号化に使用されるキーの管理プロセスおよび手順をすべて文書化し、実装する。これには、以下が含まれる。	・暗号鍵のライフサイクル（生成、配布、保存、廃棄など）ごとに適切に管理する。	4.1.4.4	
要件：4	**オープンな公共ネットワーク経由でカード会員データを伝送する場合、暗号化すること**			
要件：5	**アンチウィルスソフトウェアまたはプログラムを使用し、定期的に更新すること**			
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**			
6.1	すべてのシステムコンポーネントとソフトウェアに、ベンダ提供の最新セキュリティパッチを適用する。重要なセキュリティパッチは、リリース後 1 カ月以内にインストールする。 注: 組織は、パッチインストールの優先順位を付けるために、リスクに基づくアプローチの適用を検討できる。たとえば、重要なインフラストラクチャ（一般に公開されているデバイス、システム、データベースなど）に重要性の低い内部デバイスよりも高い優先順位を付けることで、優先順位の高いシステムおよびデバイスは 1 カ月以内に対処し、重要性の低いシステムおよびデバイスは 3 カ月以内に対処するようにする。	・最新のDBMSのセキュリティパッチを適用する。	4.1.1.1(1)	★
6.2	新たに発見された脆弱性を特定するためのプロセスを確立する（インターネット上で無料で入手可能な警告サービスに加入するなど）。新たな脆弱性の問題に対処するために、PCI DSS 要件 2.2 で要求されているとおりに構成基準を更新する。	・DBに関するセキュリティの事故や脆弱性の最新情報を常に収集する。	3.2.1(3)	
6.3	PCI DSS（安全な認証やロギングなど）に従い、業界のベストプラクティスに基づいてソフトウェアアプリケーションを開発し、ソフトウェア開発ライフサイクル全体を通して情報セキュリティを実現する。これらのプロセスには、以下を含める必要がある。			
6.3.1	導入前にすべてのセキュリティパッチ、システムとソフトウェア構成の変更をテストする（以下のテストが含まれるが、これらに限定されない）。			
6.3.1.3	暗号化による安全な保存の検証	・データ暗号化機能／ツールを利用し、格納データを暗号化する。	4.1.4.2(1)	
6.3.1.5	適切な役割ベースのアクセス制御（RBAC）の検証	・ロール、または各アカウント別に、最低でもテーブル、可能であれば列（カラム）単位でアクセス制御する。		
6.3.2	開発/テスト環境と本番環境の分離	・開発環境と本番環境は、インスタンスを分離する、可能であれば、異なるノードに作成する。	4.1.2.1(6)	★
6.3.5	本番環境システムがアクティブになる前にテストデータとテストアカウントを削除する	・DB内のテストデータ、テスト用DBアカウントを削除する。		

No.	PCI DSS要件	DBセキュリティに関する補足	DBSC ガイド	実
6.3.6	アプリケーションがアクティブになる前、または顧客にリリースされる前に、カスタムアプリケーションアカウント、ユーザー ID、パスワードを削除する	・DB内のカスタムアプリケーション用DBアカウントを削除する。		
要件：7	**カード会員データへのアクセスを、業務上必要な範囲内に制限すること**			
7.1	システムコンポーネントとカード会員データへのアクセスを、業務上必要な人に限定する。アクセス制限には以下を含める必要がある。			
7.1.1	特権ユーザー ID に関するアクセス権が、職務の実行に必要な最小限の特権に制限されていること	・管理者用DBアカウントについて、DBへのアクセス要件に基づき、必要最低限のアクセス権限を付与する。 ・管理者権限は、DBアカウントを限定して付与する。	4.1.3.1(2) 4.1.3.1(2)	★ ★
7.1.2	特権の付与は、個人の職種と職能に基づくこと	・役割ごと、利用者ごとに、適切な権限を持ったアカウントを整理する。 ・DB管理者アカウントは特定の者しか、利用できないようにする。 ・DB管理者アカウントを担当者別に割当てる。	3.1.3(2) 4.1.2.1(5) 4.1.2.1(5)	 ★ ★
7.1.4	自動アクセス制御システムを実装する	・DBMSのアクセス制御機能により、DBアカウント（またはロール）別にテーブル単位（可能であれば列単位）にアクセス制御する。		
7.2	複数のユーザーを持つシステムコンポーネントに対して、ユーザーの必要な範囲に基づいてアクセスを制限し、特に許可されていない限り「すべてを拒否」に設定した、アクセス制御システムを確立する。 アクセス制御システムには以下を含める必要がある。			
7.2.2	職種と職能に基づく、個人への特権の付与	・役割ごと、利用者ごとに、適切な権限を持ったアカウントを整理する。 ・DB管理者アカウントは特定の者しか、利用できないようにする。 ・DB管理者アカウントを担当者別に割当てる。	3.1.3(2) 4.1.2.1(5) 4.1.2.1(5)	 ★ ★
要件：8	**コンピュータにアクセスできる各ユーザに一意の ID を割り当てる。**			
8.1	システムコンポーネントまたはカード会員データへのアクセスを許可する前に、すべてのユーザに一意の ID を割り当てる。	・DBアカウントを担当者別に割当てる。(作成する)	4.1.2.1(5)	★
8.2	一意の ID の割り当てに加え、以下の方法の少なくとも 1 つを使用してすべてのユーザを認証する。 ・ パスワードまたはパスフレーズ ・ 2 因子認証（トークンデバイス、スマートカード、生体認証、公開鍵など）	・DBアカウントの認証方式を左記のいずれかにする。		
8.4	（「PCI DSS Glossary of Terms,Abbreviations, and Acronyms」で定義されている）強力な暗号化を使用して、すべてのシステムコンポーネントでの伝送および保存中にすべてのパスワードを読み取り不能にする。	・一般的な商用DBMSなら問題なし		
8.5	すべてのシステムコンポーネントで、以下のように、消費者以外のユーザおよび管理者に対して適切なユーザ認証とパスワード管理を確実に行う。			
8.5.3	初期パスワードをユーザごとに一意の値に設定し、初回使用後に直ちに変更する。	・DBMSの機能により、初期パスワードを強制的に変更させる設定でDBアカウントを作成する。	4.1.2.2(2)	★
8.5.4	契約終了したユーザのアクセスは直ちに取り消す。	・契約終了した担当者用のDBアカウントを削除する。	4.1.2.1(2)	★
8.5.5	少なくとも 90 日ごとに非アクティブのユーザアカウントを削除/無効化する。	・少なくとも90日ごとに不要なDBアカウントを削除または無効化する。	4.1.2.1(3)	★
8.5.6	リモート保守のためにベンダが使用するアカウントは、必要な期間のみ有効にする。	・一時的な利用者にはその都度、DBアカウントに対し一時的なパスワードを与える。	4.1.2.2(7)	★
8.5.8	グループ、共有、または汎用のアカウントおよびパスワードを使用しない。	・DBアカウントを担当者別に割当てる。(作成する)	4.1.2.1(5)	★
8.5.9	少なくとも 90 日ごとにユーザパスワードを変更する。	・少なくとも90日ごとにDBアカウントのパスワードを変更する。	4.1.2.2(2)	★
8.5.10	パスワードに 7 文字以上が含まれることを要求する。	・DBMSの機能により、パスワードの複雑性を設定する。	4.1.2.1(1)	★
8.5.11	数字と英文字の両方を含むパスワードを使用する。	・DBMSの機能により、パスワードの複雑性を設定する。	4.1.2.1(1)	★
8.5.12	ユーザが新しいパスワードを送信する際、最後に使用した 4 つのパスワードと同じものを使用できないようにする。	・DBMSの機能により、利用可能なパスワード履歴を設定する。		
8.5.13	最大 6 回の試行後にユーザ IDをロックアウトして、アクセス試行の繰り返しを制限する。	・DBMSの機能により、ロックアウトを設定する。	4.1.2.1(4)	★
8.5.14	ロックアウトの期間を、最小 30分または管理者がユーザ ID を有効にするまで、に設定する	・DBMSの機能により、ロックアウトを設定する。	4.1.2.1(4)	★
8.5.15	セッションが 15 分を超えてアイドル状態の場合、端末を再有効化するためにユーザにパスワードの再入力を要求する。	・DBMSの機能により、アイドル時間を設定する。		
8.5.16	カード会員データを含むデータベースへのすべてのアクセスを認証する。これには、アプリケーション、管理者、およびその他のすべてのユーザによるアクセスが含まれる。	・一般利用者はアプリケーション経由でのみデータにアクセスできるようにし、アプリケーションは利用者を認証、認可を適切に実施する。 ・DBに直接アクセスできるのは、DB管理者に限定する。		
要件：9	**カード会員データへの物理アクセスを制限する。**			
要件：10	**ネットワークリソースおよびカード会員データへのすべてのアクセスを追跡および監視する。**			
10.2	以下のイベントを再現するためにすべてのシステムコンポーネントの自動監査証跡を実装する。			
10.2.1	カード会員データへのすべての個人アクセス	・ＤＢに対するすべてのアクセスを記録する。	4.2.1.1(2)	★
10.2.2	ルート権限または管理権限を持つ個人によって行われたすべてのアクション	・ＤＢに対するDB管理者によるすべてのアクセスを記録する。	4.2.2.3(2)	★
10.2.3	すべての監査証跡へのアクセス	・DB監査証跡に対するすべてのアクセスを記録する。		
10.2.4	無効な論理アクセス試行	・ＤＢに対する以下のような無効な論理アクセスを記録する。 例) ・SQL構文エラー ・存在しないオブジェクトに対するアクセス ・権限のないオブジェクトに対するアクセス		
10.2.5	識別および認証メカニズムの使用	・DBに対するログイン／ログアウトを記録する。	4.2.1.1(1)	★
10.2.6	監査ログの初期化	・DB監査証跡の初期化、設定変更などの操作を記録する。		
10.2.7	システムレベルオブジェクトの作成および削除	・DBオブジェクト（DBアカウント、テーブル、ビュー など）の作成、変更などの操作を記録する。	4.2.1.1(4)	★

No.	PCI DSS要件	DBセキュリティに関する補足	DBSC ガイド	実
10.3	イベントごとに、すべてのシステムコンポーネントについて少なくとも以下の監査証跡エントリを記録する。			
10.3.1	ユーザ識別	・DBアカウント名（ID）、OSアカウント名、アプリケーションアカウント名など		
10.3.2	イベントの種類	・SQL文、SQLタイプ		
10.3.3	日付と時刻	・操作日時		
10.3.4	成功または失敗を示す情報	・操作結果、エラーコード		
10.3.5	イベントの発生元	・DBクライアントのIPアドレス、マシン名など		
10.3.6	影響を受けるデータ、システムコンポーネント、またはリソースの ID または名前	・オブジェクト名、オブジェクトID、カラム名、カラムIDなど		
10.5	変更できないよう、監査証跡をセキュリティで保護する。			
10.5.1	監査証跡の表示を、仕事関連のニーズを持つ人物のみに制限する。	・DB監査証跡にアクセスできる人物を最小限に制限する。	4.2.1.2(1)	★
10.5.2	監査証跡ファイルを不正な変更から保護する。	・DB監査証跡にアクセスできる人物を最小限に制限する。 ・DB監査証跡の改ざん対策を講じる。 例） ・ログの多重化 ・電子証明書（タイムスタンプなど）の付加	4.2.1.2(1) 4.2.1.2(2)	★ ★
10.5.3	監査証跡ファイルを、変更が困難な一元管理ログサーバまたは媒体に即座にバックアップする。	・DB監査証跡を左記の運用で管理する。 例） ・書き換え不能ストレージの使用	4.2.1.2(2)	★
10.5.5	ログに対してファイル整合性監視または変更検出ソフトウェアを使用して、既存のログデータを変更すると警告が生成されるようにする（ただし、新しいデータの追加は警告を発生させない）。	・DB監査証跡の改ざん対策を講じる。	4.2.1.2(2)	★
10.6	少なくとも日に一度、すべてのシステムコンポーネントのログを確認する。ログの確認には、侵入検知システム（IDS）や認証、認可、アカウンティングプロトコル（AAA）サーバ（RADIUS など）のようなセキュリティ機能を実行するサーバを含める必要がある。 注: 要件 10.6 に準拠するために、ログの収集、解析、および警告ツールを使用することができます。	・DBにおいても、ログ解析・検知ツールを使用して、少なくとも日に一度、DB監査証跡の内容を確認し不審な操作を検出する。	4.2.2 4.2.3	★ ★
10.7	監査証跡の履歴を少なくとも 1 年間保持する。少なくとも 3 カ月はすぐに分析できる状態にしておく（オンライン、アーカイブ、バックアップから復元可能など）。	・DB監査証跡を少なくとも1年間保持する。 ・少なくとも3ヶ月は、すぐにDB監査証跡を分析できる状態にしておく。		
要件：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。**			
11.2	内部および外部ネットワークの脆弱性スキャンを少なくとも四半期に一度およびネットワークでの大幅な変更（新しいシステムコンポーネントのインストール、ネットワークトポロジの変更、ファイアウォール規則の変更、製品アップグレードなど）後に実行する。 注: 四半期に一度の外部の脆弱性スキャンは、PCI（Payment Card Industry）セキュリティ基準審議会（PCI SSC）によって資格を与えられた ApprovedScanningVendor(ASV) によって実行される必要があります。ネットワーク変更後に実施されるスキャンは、会社の内部スタッフによって実行することができます。	・DBサーバ(OSレベル、DBMS製品)、及びデータが格納されるインスタンスに対して、少なくとも四半期に一度脆弱性をスキャンする。	4.1.6.3(1)	
11.3	外部および内部のペネトレーションテストを少なくとも年に一度および大幅なインフラストラクチャまたはアプリケーションのアップグレードや変更（オペレーティングシステムのアップグレード、環境へのサブネットワークの追加、環境への Web サーバの追加など）後に実行する。これらのペネトレーションテストには以下を含める必要がある。			
11.3.2	アプリケーション層のペネトレーションテスト	・DBサーバ(OSレベル、DBMS製品)、及びデータが格納されるインスタンスに対して、少なくとも年に一度ペネトレーションテストを実施する。		
要件：12	**従業員および派遣社員向けの情報セキュリティポリシーを整備する。**			
12.1	以下を実現するセキュリティポリシーを確立、公開、維持、および周知する。			
12.1.2	脅威、脆弱性、結果を識別する年に一度のプロセスを正式なリスク評価に含める。	・DBセキュリティ対策の有効性を評価する。	3.1.2	
12.1.3	レビューを少なくとも年に一度含め、環境の変化に合わせて更新する。	・環境の変化に合わせてDBアカウントを見直す。 例） ・不適切なアカウントや権限を再度整理する。	3.1.3(3)	
12.2	この仕様の要件と整合する日常的な運用上のセキュリティ手順を作成する（たとえば、ユーザアカウント保守手順、ログレビュー手順）。	・DB管理業務のチェック。 例） ・管理業務の記録を残す。 ・管理者のローティーションを実施する。	3.2.1(3)	
12.5	個人またはチームに以下の情報セキュリティ管理責任を割り当てる。			
12.5.4	追加、削除、変更を含め、ユーザアカウントを管理する	・DBアカウント管理する。 例） ・DB利用者の整理。 ・DBアカウントの整理。	3.1.3(1) 3.1.3(2)	
12.5.5	データへのすべてのアクセスを監視および管理する。	・DBアクセスログを監視および管理する。 例） ・ログの取得の目的。 ・ログ取得対象アクセスの整理。	3.1.4	

[補足説明]
DBSCガイド：『データベースセキュリティガイドライン 第2.0版』の項番リンク
実　　：『DBセキュリティ 製品別機能対応表』が対応している項目の場合、『★』を記載