COALFIRE

ORACLE MINICLUSTER：PCIとSOC2に関するコンプライアンス・レビュー

認定セキュリティ評価機関による評価

2016年10月31日

Coalfire、シニア情報セキュリティ・コンサルタント、Allen Mahaffy

COALFIRE

内容

COALFIRE

概要

Oracle MiniCluster S7-2（Oracle MiniCluster）は、さまざまなデータベース・アプリケーションやエンタープライズ・アプリケーションを実行する多目的のエンジニアド・システムです。業界固有のセキュリティ要件に対応した事前構成済みセキュリティ制御機能を使用して包括的に情報セキュリティに対処します。また、組織やクラウド・サービス・プロバイダ内でホストされるセキュリティ要件の厳しいアプリケーションを実行するため、コンプライアンスに対応した環境を提供します。

ペイメントカードデータを処理、伝送、保存する組織は、PCI DSS（Payment Card Industry Data Security Standard：ペイメントカード業界セキュリティ基準）を継続的に遵守する必要があります。このセキュリティ要件を満たすには、ペイメントカード情報を処理、保存、伝送するネットワークやシステムを構成するすべてのコンポーネントにセキュリティ対策を施す必要があります。ペイメントカード・サービス・プロバイダはもちろん加盟店も、年に一度、PCI DSS要件に準拠していることを証明する必要があります。本書は、組織がアプリケーションやデータベースのセキュリティ強化を必要としている場合に、Oracle MiniClusterで対応可能なPCI DSSの該当要件を、こうした加盟店やサービス・プロバイダに明らかにすることを目的としています。

また、サービス・プロバイダは、主要サービスを適切に管理していることを示す客観的な保証を顧客や見込み顧客に提供するよう定期的に要求されます。この客観的保証を提供するもっともよい方法の1つは、SOC2 Type2報告書を徹底することです。SOC2 Type2報告書は、システムがユーザーに及ぼす可能性のある運用上およびコンプライアンス上のリスクを軽減するために、サービス・プロバイダが効果的なシステム管理を導入しているという信用と保証を届けるためのものです。さらに、PCI DSSの要件には、SOC2 Type 2 Trustサービス基準を満たす管理項目が多数含まれています。本書には、Oracle MiniClusterで適合または対応可能なPCI 3.2の要件と、同様に対応可能なSOC2基準との対応関係を掲載しました。

はじめに

本書は、カード会員データ環境（CDE）または本番環境にOracle MiniClusterを実装するIT専門家や、それらを評価することを任務とする認定セキュリティ評価機関（QSA）またはIT監査人に情報を提供することを目的としています。Oracle MiniClusterの機能、コンプライアンス・テストの結果、および公表されている制御機能をPCI DSS 3.2の要件およびSOC2の基準と比較し、コンプライアンス要件への適合性を分析しました。詳細説明の項には、これらの制御機能がどのようにPCI要件に準拠するかをまとめています。

簡潔な文書にするために、Oracle MiniCluster製品の使用とは無関係の要件、特長、制御機能は、詳しい分析から除外しました。Oracle MiniClusterの制御機能のテストはCoalfireが独自に実施したものではありません。本書に書かれている意見は、オラクルが公開している情報源から取得した文書に記載されているOracle MiniClusterの特長と制御機能に対するCoalfireの見解です。

Oracle MiniClusterは、複数の仮想アプリケーションやデータベースをホスティングする単一テナントを想定したものです。おもなセキュリティ機能は次のとおりです。

- ネットワークの分離とデータ・リンクの保護
- 多層アクセス制御
- 鍵の一元管理（PKCS#11、KMIP）
- 監視および監査
- コンピューティング層、ストレージ層、ネットワーク層、データベース層、アプリケーション層全体の包括的なデータ保護機能

PCI DSS v3.2の多数の要件に適合または対応するPCI DSSプロファイルを選択すると、インストール時にOracle MiniClusterの統合セキュリティ機能が事前構成されます。さらに、サービス・プロバイダや企業顧客は、単一テナント・サービスまたはクラウド・アーキテクチャ内の専用コンピューティング環境に対応するように事前構成したOracle MiniClusterを使用して、規定の要件を満たすことができます。企業もクラウド・サービス・プロバイダも、特に両者に適用される多様なPCI DSS要件に適合または対応できます。

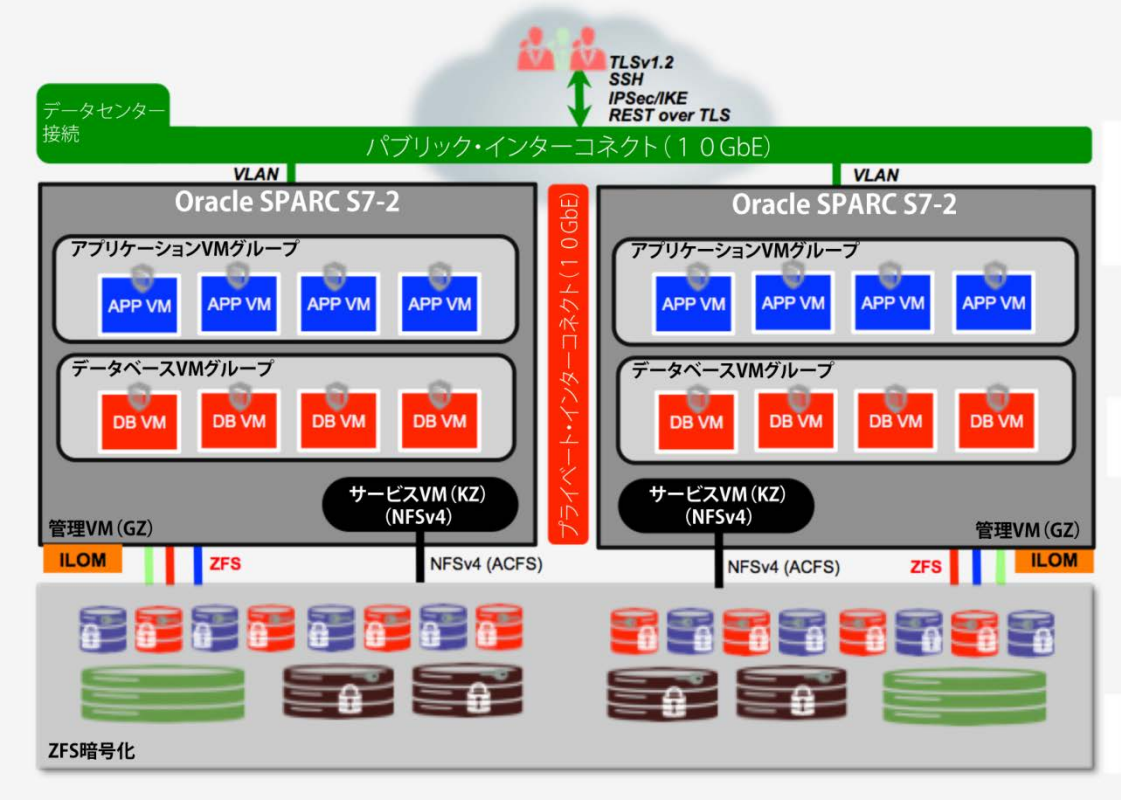

図1：Oracle MiniClusterのアーキテクチャ

ペイメントカード業界のデジタル・セキュリティ基準

PCI DSSは、カード会員データを処理、保存または伝送するコンピュータ・システム環境の保護に必要な最小限の情報セキュリティ制御を実現する情報セキュリティ要件のフレームワークです。

カード会員データ（ペイメントカードデータ）を処理、保存または伝送する組織はPCI DSSを遵守する必要があり、年に一度、コンプライアンス状況を証明する必要があります。現時点で遵守が必要なのは、2016年10月発効のPCI DSSバージョン3.2です。

PCI DSSフレームワークは12の要件で構成されており、それぞれの要件に複数の下位要件（管理項目）があり、管理項目とその検証手順はそこに詳しく記述されています。PCI DSSは、組織がカード会員データ環境（CDE）を定義することと、組織のカード会員データ環境または確立されたサンプリングに対してPCI DSS要件を評価することを義務づけています。

安全なネットワークおよびシステムの構築と維持

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

Oracle MiniClusterは、この要件に関連する複数のセキュリティ制御に適合または対応するようにあらかじめ構成されています。たとえば、Oracle MiniClusterは、着信および発信ネットワークパケットがSolarisのIPフィルタまたはパケット・フィルタを介して仮想マシンまたはアクセス制御リスト（またはその両方）でフィルタリングされるよう、あらかじめ構成されています。ネットワーク・ファイアウォール機能には、ステートフル・パケット・フィルタリング、ネットワーク・アドレス変換、ポート・アドレス変換などがあります。仮想マシンを導入すると、Oracle MiniClusterのデフォルト・ファイアウォール・ポリシーによりデフォルトの「deny-all」（すべて拒否）に設定されます。また、クライアント・アクセス・ネットワーク・トラフィックは、IPsec/IKEを使用する暗号化により保護されます。

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ー提供のデフォルト値を使用しない

Oracle MiniClusterは、米国防総省が公開している基準（DoDセキュリティ技術導入ガイド）や米国インターネット・セキュリティ・センター（CIS）のベンチマークをはじめとする多様なセキュリティ構成基準に準拠するように構成でき、納入プロセスの一環として、すべてのデフォルト・パスワードを顧客のみが知る値に変更することができます。

カード会員データの保護

3.保存されるカード会員データを保護する

カード会員データを保存する組織を想定し、Oracle MiniClusterには、この要件の複数の管理項目に適合または対応するように構成できる統合セキュリティ制御機能が実装されています。また、コンピュート、ネットワーク、ストレージおよびデータベースの各レベルでカード会員データを厳密に分離する安全な分離テクノロジーが組み込まれています。これらの機能を必要に応じて組み合わせることで、アーキテクチャ、ワークロードおよびセキュリティにかかわる多様な要件に対応することができます。さらに、強力な認証とロールベースのアクセス制御テクノロジーを使用することで、権限を有する個人とサービス以外はカード会員データにアクセスできないようにすることができます。加えて、ネットワークを経由してデータベースまたはディスクに保存されるカード会員データは、強力な暗号化を使用して保護されます。強力な暗号化は解読不能と考えられており、NISTに承認された暗号アルゴリズムでもあります。これらの制御を併用することで、機密性の高いカード会員情報の機密保護と整合性を確保できます。

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

Oracle MiniClusterは、プラットフォームを出入りするカード会員データが強力な暗号化手段によって保護されるよう、あらかじめ構成されています。Oracle MiniClusterで処理される機密性の高いデータがネットワーク上を流れるときは必ず暗号化されるようにするために、TLS（SSL）、SSH、IPsecなど、すべてのプロトコルが使用されます。これらの機能の対象には、アプリケーションとカード会員データだけでなく、Oracle MiniClusterプラットフォームの管理と監視に使用されるプロトコルとサービスも含まれます。

脆弱性管理プログラムの整備

5.すべてのシステムをマルウェアから保護し、ウイルス対策ソフトウェアまたはプログラムを定期的に更新する

PCI DSSは、「悪意のあるソフトウェアの影響をうけやすいすべてのシステムに、ウイルス対策ソフトウェアを導入すること」を義務づけています。Oracle MiniClusterはこの要件を満たしませんが、いくつかの方法で準拠できています。たとえば、Oracle MiniClusterは、Oracle Solarisオペレーティング・システムが稼働するコンピュート・ノード上に構築されています。Oracle Solarisオペレーティング・システムは、ZFSファイル・システムに保存されるコンテンツに対してリアルタイムでマルウェア対策スキャンを実施するVSCANサービスに対応しています。VSCANサービスは、業界標準のICAPプロトコルを使用して外部サーバーと統合されます。これに加え、Oracle MiniClusterは、セキュア・ベリファイド・ブート、不変非大域ゾーン、ハードウェア支援型シリコン・セキュアド・メモリ、実行不能スタック、アドレス空間配置のランダム化、データ・リンク保護など、統合された複数のマルウェア対策機能をサポートしています。まとめると、これらのセキュリティ制御機能により、Oracle MiniCluster上で非常に整合性のとれた環境を構築できます。

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

この要件の管理項目では、開発/テスト環境と本番環境とで責務を分離することを求めていますが、Oracle MiniClusterはこの管理項目に適合または対応することができます。Oracle MiniClusterは、脆弱性を管理するプログラムの整備や、ベンダーが提供するセキュリティ・パッチのすみやかな適用を求めたその他の管理項目についても対応しています。Oracle MiniClusterに元来組み込まれているセキュリティ制御機能にオラクルのCritical Patch UpdatesとSecurity Alertsを組み合わせることで、安全なマルチテナント設計や単一テナント設計を実現できます。

強固なアクセス制御方法の導入

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

Oracle MiniClusterには、強力な認証の他に、コンピュート、ストレージ、ネットワーク、データベースのすべてのコンポーネントを対象にしたユーザーとロールに基づくアクセス制御が組み込まれています。また、これらのコンポーネントにアクセス制御ポリシーを適用することで、権限を有するユーザー以外は機密情報や機能にアクセスできないようにすることができます。これにより、Oracle MiniClusterのアクセス制御機能は、この要件の管理項目（下位要件）の多くに適合または対応することができます。

8.コンピュータにアクセスできる各ユーザーに一意のIDを割り当てる

Oracle MiniClusterは、この要件に含まれる管理項目の多くに適合または対応するようにあらかじめ構成されています。より重要なのは、カード会員データを保存、処理または伝送する顧客を有するサービス・プロバイダに対してPCI DSSが課している、追加のアクセス制御要件に適合するように構成することもできるという点です。

Oracle MiniClusterに統合されている権限を最小限に絞ったユーザーベース・アクセス制御とロールベース・アクセス制御（RBAC）を使用して、コンピュート、ストレージ、ネットワーク、データベースおよびアプリケーションの各サービスへのアクセスを制御および制限できます。これらの細かな設定の可能なアクセス制御を使用することで、マルチテナント環境でも単一テナント環境でも、管理権限の適用範囲と使用を最小限に抑えることができます。

9.カード会員データへの物理アクセスを制限する

Oracle MiniClusterは、データ保護ライフサイクルを事前構成し、検出機能が強化された、包括的なデータ保護ライフサイクル制御が可能な場所に情報資産を統合することで、この要件に対応できます。

定期的なネットワークの監視およびテスト

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

Oracle MiniClusterに元来組み込まれている監査/監視機能は、すべてのコンピュート、ストレージ、ネットワーク、データベース、アプリケーション資産にわたって管理操作と管理処理を監視するよう事前構成されているため、この要件に詳述されている多数の管理項目に適合または対応しています。これは、単一テナント・ソリューションとして構成されたOracle MiniClusterや、PCI DSS付録Aのサービス・プロバイダ向け要件で義務づけられている顧客のセグメント化が可能なマルチテナント・アーキテクチャ内に統合されたOracle MiniClusterでも同じです。

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

Oracle MiniClusterにIDS/IPSシステムや変更検出機能は事前構成されていませんが、IDS/IPSセンサーを統合するか、ホストベースのソリューションを利用することで、Oracle MiniClusterの上流で着信および発信するトラフィックを監視することができます。変更検出機能を補う管理項目を満たすために、Oracle MiniClusterには基本監査報告機能（BART）、ベリファイド・ブート、強固なアクセス制御を利用したカスタムのファイル変更監視機能があります。

12 .すべての担当者の情報セキュリティ・ポリシーを整備する

この要件に詳述されている管理項目のおもな対象は、PCI DSSの要件と情報セキュリティのベスト・プラクティスを実施するために必要なプロセス、ポリシーおよび手順にかかわる制御です。そのため、Oracle MiniClusterはこの要件に直接的には適合または対応しません。

要件A.1：共有ホスティング・プロバイダは、カード会員データ環境を保護すること

付録Aに詳述されているように、PCI DSSにはサービス・プロバイダのみに適用される要件が含まれていますが、企業ユーザーはOracle MiniClusterの統合アクセス制御、データ保護、監視/監査機能を利用することでこれらの要件に適合または対応できます。そのため、マルチテナント・ホスティング・ソリューションのサービス・プロバイダに対してPCI DSSが要求する重要情報に差があっても問題ありません。

COALFIRE

PCI DSS v3.2の詳細説明

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

ファイアウォールは、事業体のネットワーク（内部）と信頼できないネットワーク（外部）との間で許可されたコンピュータ・トラフィックはもちろん、事業体の信頼できる内部ネットワークの中の機密性のより高い領域を出入りするトラフィックを制御するデバイスです。カード会員データ環境は、事業体の信頼できるネットワークの中でも一段と機密性の高い領域の一例です。

Oracle MiniClusterのホストベースのステートフル・パケット・インスペクション・ファイアウォールは、PCI DSSの要件1に含まれる管理項目の多くに適合または対応するようあらかじめ構成されています。顧客は、カスタム・アプリケーションのポートとプロトコルの特定が必要になる場合があります。Oracle MiniClusterには、多重防御アーキテクチャに利用できるさまざまな階層型セキュリティ制御機能が用意されています。また、Oracle MiniClusterでは、レイヤー2またはレイヤー3でのネットワーク分離、アクセス制御、ステートフル・ファイアウォール暗号化（IPsec、SSL/TLS）の促進や、VLANのトランスポート層のアクセスリストの適用も容易です。

PCI要件	Oracle MiniClusterの詳細	適合または対応
1.2 信頼できないネットワークとカード会員データ環境内のすべてのシステム・コンポーネントの接続を制限する、ファイアウォールとルーターの構成を構築する。	Oracle MiniClusterでは、SolarisのIPフィルタを介したホストベースのファイアウォール・パケット・フィルタリングにより、公開されているサービスへのネットワーク・アクセスを制限できます。IPフィルタは、仮想マシン・レベルまたはアクセス制御リスト（または両方）で着信および発信ネットワーク・トラフィックのポリシーを適用し、物理デバイスと仮想デバイスとの間の通信を制限できます。	対応
1.2.1 着信および発信トラフィックを、カード会員データ環境に必要なトラフィックにし、それ以外のすべてのトラフィックを特定的に拒否する。	Oracle SolarisのIPフィルタが、着信および発信トラフィックを必要なトラフィックのみに制限するようあらかじめ構成されており、デフォルトは、導入されている仮想マシン上のトラフィックをすべて拒否（deny-all）するように構成されています。	対応または適合
1.2.3 すべてのワイヤレス・ネットワークとカード会員データ環境の間に境界ファイアウォールをインストールし、ワイヤレス環境とカード会員データ環境間のトラフィックを拒否または、業務上必要な場合、承認されたトラフィックのみを許可するようにファイアウォールを構成する。	Oracle SolarisのIPフィルタをステートフル・パケット・インスペクション・ファイアウォールとして利用すると、Oracle MiniCluster外のすべてのワイヤレス・ネットワークとOracle MiniCluster上のすべてのカード会員データ環境ネットワークをファイアウォールで分離できます。アクセスが必要な場合は、Oracle MiniClusterのステートフル・ファイアウォールで、どのネットワーク・ベースのステートフル・パケット・インスペクション・ファイアウォールとも同じように非常にきめ細かくカード会員データ環境へのアクセスを設定できます。	対応
1.3 インターネットとカード会員データ環境内のすべてのシステム・コンポーネント間の、直接的なパブリック・アクセスを禁止する。	Oracle SolarisのIPフィルタをネットワーク・ベースのファイアウォールまたは境界ルーターのファイアウォール機能およびアクセス制御リストと組み合わせることで、カード会員データ環境との間の直接的なアクセスをすべて禁止することができます。	対応
1.3.4 カード会員データ環境からインターネットへの不正な発信トラフィックを禁止する。	Oracle MiniClusterのホストベースのIPフィルタ・ステートフル・パケット・インスペクション・ファイアウォールが、認可されたトラフィックのみカード会員データ環境からインターネットに発信されるように、出口アクセス制御リストを使用してあらか	適合

	じめ構成されています。	
1.3.5 ネットワーク内へは、「確立された」接続のみ許可する。	Oracle MiniClusterのIPフィルタ・ステートフル・パケット・インスペクション・ファイアウォールが、この要件に適合するようにあらかじめ構成されています。イーサネットを介したステートフル・パケット・フィルタリングがサポートされています。	適合
1.3.6 DMZやその他の信頼できないネットワークから隔離されている内部ネットワーク・ゾーンで、カード会員データを保存するコンポーネント（データベース）が実装されている。	Oracle MiniClusterのIPフィルタ・ステートフル・パケット・インスペクション・ファイアウォールが、この要件に適合するようにあらかじめ構成されています。	適合
1.3.7 プライベートIPアドレスとルーティング情報を許可されていない第三者に開示しない。 注：IPアドレスを開示しない方法には、以下のものが含まれるが、これらに限定されるわけではない： • ネットワーク・アドレス変換（NAT） • カード会員データを保持するサーバーをプロキシサーバー/ファイアウォールの背後に配置する。 • 登録されたアドレス指定を使用するプライベート・ネットワークのルート・アドバタイズを削除するか、フィルタリングする。 • 登録されたアドレスの代わりにRFC1918アドレス空間を内部で使用する。	権限を持たない第三者にプライベートIPアドレスやルーティング情報が開示されないようにするために、ネットワーク・アドレス変換とポート・アドレス変換を実行するよう、Oracle MiniClusterのIPフィルタがあらかじめ構成されています。	適合
1.4 インターネットに直接接続するポータブル・コンピュータ・デバイス（会社あるいは従業員が所有のものも含む）で、ネットワークの外側ではインターネットに接続され、またCDEへのアクセスにも使用されるものに（従業員が使用するラップトップなど）、パーソナル・ファイアウォール・ソフトウェアか同等機能のソフトウェアをインストールする。ファイアウォール（またはそれに相当する）構成には以下が含まれます。 • 特定の構成設定が定義されている。 • パーソナル・ファイアウォール（またはそれに相当する機能）がアクティブに実行中である。 • パーソナル・ファイアウォール（またはそれに相当する機能）がモバイル・デバイスのユーザーによって変更できないようになっている。	ホストされている仮想ゲスト・コンピュータには、Oracle SolarisのIPフィルタ・ファイアウォールがホストベースのファイアウォールとしてあらかじめインストールされています。事前定義された固有の構成設定一式はあらかじめ構成されており、ファイアウォールは常時稼働し、ユーザーはファイアウォールの構成を変更できないようになっています。	適合

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ー提供のデフォルト値を使用しない

悪意のある個人（事業体の内外を問わず）が、ベンダー提供のデフォルト・パスワードやその他のデフォルト設定を使用してシステムに侵入することがよくあります。これらのパスワードや設定はハッカー・コミュニティでよく知られており、公開情報によって容易に特定できます。

Oracle MiniClusterは、PCI-DSS 3.2専用のパスワード・ポリシーと認証ポリシーを使用してあらかじめ構成されています。

PCI要件	Oracle MiniClusterの詳細	適合または対応
2.1 システムをネットワーク上に導入する前に、必ずベンダー提供のデフォルト値を変更し、不要なデフォルト・アカウントを無効にする。 これは、オペレーティング・システム、セキュリティ・サービスを提供するソフトウェア、アプリケーション、システム・アカウント、POS端末、ペイメント・アプリケーション、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で使用されるが、これらに限定されない、すべてのデフォルト・パスワードに適用されます。	Oracle MiniClusterに組み込まれている一部のオラクル製品は、デフォルトの管理パスワードを設定した状態で納品されるため、使用する前に変更する必要があります。 セキュリティ・ガイドを参考にして、組織の構成基準に合わせて構成をカスタマイズしてください。 Oracle MiniClusterをインストールすると、ほとんどのネットワーク・サービスは「デフォルトでのセキュリティ強化」機能によって無効化され、SSH以外ではリモート・アクセスができなくなります。	対応または適合
2.2.1同じサーバーに異なったセキュリティ・レベルを必要とする機能が共存しないように、1つのサーバーには、主要機能を1つだけ実装する。（たとえば、Webサーバー、データベース・サーバー、DNSは別々のサーバーに実装する必要がある。）	オラクルの仮想化テクノロジーを使用すると、1つの主要機能だけを提供する仮想ホストを作成することができます。 Oracle MiniClusterのコンプライアンス・レポート機能は、ベンチマークをテストしてコンプライアンスの成否を示す報告書を作成する機能です。	対応または適合
2.2.2 システムの機能に必要なサービス、プロトコル、デーモンなどのみを有効にする。	Oracle Solarisには「デフォルトでのセキュリティ強化」機能があるため、不要なサービス、プロトコル、デーモン/サーバーは決して実行されず、SSH以外のプロトコルではリモート接続のリッスンは行われず、ローカル・アクセス以外は権限を昇格することができません。	対応または適合
2.2.3 安全でないとみなされている必要なサービス、プロトコル、またはデーモンに追加のセキュリティ機能を実装する。	Oracle MiniClusterはデフォルトでセキュアなサービスのみを利用するため、Oracle MiniClusterをデフォルト構成で使用する場合はセキュリティ機能を追加する必要はありません。セキュアでないサービス、プロトコル、またはデーモン（サーバー）のセキュリティを強化するために防御層を追加する場合は、この要件に適合または対応するためにPCI-DSSセキュリティ・プロファイルをインストール時に選択することで、アクセス制御、ステートフル・パケット・インスペクション、セキュア・ゾーンの隔離、強力な認証およびロギングを事前構成することができます。	適合

2.2.5 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、および不要なWebサーバーなど、すべての不要な機能を削除する。	攻撃の対象となる範囲を狭めるOracle MiniClusterの「デフォルトでのセキュリティ強化」機能により、多数のネットワーク・サービスをひとまとめにした形で不要な機能を無効化し、ローカル以外ではアクセス権を高くすることができないようにしています。また、着信ネットワーク接続はSSHでのみ可能です。Oracle Solarisには、デフォルトで接続をリッスンするWebサーバーがありません。	適合
2.3 強力な暗号化を使用して、すべてのコンソール以外の管理アクセスを暗号化する。	Oracle MiniCluster Virtual AssistantではTLS 1.2またはSSHを使用して機密情報の漏洩や管理用接続の乗っ取りを防止します。	対応または適合
2.6 共有ホスティング・プロバイダは、各事業体のホスト環境およびカード会員データを保護する必要がある。これらのプロバイダは、付録A1：「共有ホスティング・プロバイダでの追加PCI DSS要件」に示されているように、特定の要件を満たす必要がある。	Oracle MiniClusterの統合監視、アクセス制御、および暗号化は、セキュアな分離テクノロジーと組み合わせることで、付録A：「共有ホスティング・プロバイダ向けのPCI DSS追加要件」を確実に遵守するように設計および構成できます。	対応

要件3：保存されるカード会員データを保護する

暗号化、切捨て、マスキング、ハッシュなどの保護方法は、カード会員データを保護するための重要なコンポーネントです。たとえ侵入者がセキュリティ制御を巧みに逃れて、暗号化されたデータにアクセスできたとしても、正しい暗号化キーがなければ、データを読み取り、使用することはできません。保管したデータを保護するその他の効果的な方法も、潜在的なリスク軽減の機会として考える必要があります。たとえば、リスクを最小化する方法には、絶対に必要でない限りカード会員データを保存しないこと、プライマリ・アカウント番号（PAN）の全桁が必要でない場合はデータの端を切り捨てること、エンドユーザーメッセージング・テクノロジー（電子メールやインスタント・メッセージングなど）を使用して、保護されていないPANを送信しないことが挙げられます。

カード会員データを保存する組織はいずれも、PCI DSS要件3の該当する管理項目をすべて適用しておく必要があります。Oracle MiniClusterには、データベース内のデータを透過的データ暗号化（TDE）で暗号化する機能や、ZFSファイル・システムに保管されているデータを暗号化する機能が搭載されています。オプション機能を使用すれば、ハードウェア・セキュリティ・モジュール（HSM）またはOracle Key Managerを統合して暗号化鍵を管理することもできます。

PCI要件	Oracle MiniClusterの詳細	適合または対応
3.2 承認後に機密認証データを保存しない（暗号化されている場合でも）。機密認証データを受け取った場合、認証プロセスが完了し次第すべてのデータを復元不能にする。以下の場合に、データが安全に保存される場合は、発行者と企業が、機密認証データを保存するため、発行サービスをサポートすることが可能である。 • 業務上の理由がある • データが安全に保存されている	PCI DSSは機密認証データの保存を厳格に禁止していますが、業務上の正当な理由があって保存する必要がある場合や、組織が発行者であったり発行業務をサポートしていたりすることから保存する必要がある場合がまれにあります。業務上の正当な理由があって機密認証データを保存しなければならない場合は、Oracle MiniClusterを利用すればすべての機密情報が暗号化されます。Oracle MiniClusterでは、データベース表領域の透過的データ暗号化（TDE）か、ファイル・システムのセキュリティを確保するデフォルトのZFSベースのディスク暗号化の一方または両方を使用できます。	対応または適合

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、ログのデータを含む） • 強力な暗号化をベースにしたワンウェイ・ハッシュ（PAN全体をハッシュする必要がある） • トランケーション（PANの切り捨てられたセグメントの置き換えにはハッシュを使用できない） • 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	Oracle MiniClusterでは、データベース内のデータをTDEで暗号化（ファイルレベルまたは列レベルのデータベース暗号化）する場合や、保管されているデータにZFSディスク暗号化を適用する場合に、複数の暗号化アルゴリズムと鍵の強度を利用できます。TDEもZFS暗号化も、この項目の制御に準拠する方法で実装できます。Oracle Databaseを利用して、データ全体またはデータのほんの一部が固定値またはマスク値で置き換えられるようにすることができます。	適合
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・システムの認証および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・データベースや一般的なネットワーク・ログイン資格情報を使用しないなどの方法で）。復号キーがユーザー・アカウントと関連付けられていない。	ZFS暗号化は、ユーザー・アカウントと関連付けられない方法でディスク暗号化が実装されるように、最初のインストール時に事前構成されます。Oracle MiniClusterには、「Oracle Key Manager」をネットワークHSMアプライアンスとして使用して暗号化アクセラレーションのシームレスな提供や暗号化キー管理機能のオフロードを可能にする構成の統合を支援する機能があります。また、複数のサード・パーティ製HSM製品と統合して、暗号化キー管理機能をオフロードしたり暗号化アクセラレーションを提供したりすることもできます。	適合
3.5.3 カード会員データの暗号化/復号化に使用される秘密キーは、以下のいずれかの形式（複数可）で常時保存する。 • 少なくともデータ暗号化キーと同じ強度のキー暗号化キーで暗号化されており、データ暗号化キーとは別の場所に保存されている • 安全な暗号化デバイス（ホスト・セキュリティ・モジュール（HSM）またはPTS承認の加盟店端末装置など） • 業界承認の方式に従う、少なくとも2つの全長キーコンポーネントまたはキー共有として	Oracle MiniClusterには、ZFS暗号化キーやデータベース固有のキー、アプリケーション固有のキーを保存するための、PKCS#11ベースの一元化されたキーストアがあらかじめ構成されています。また、PKCS#11またはKMIPのインタフェースを使用するHSMへの移行準備を支援する機能があります。	対応または適合
3.5.4 暗号化キーを最小限の場所に保存する。		
3.6.1 強力な暗号化キーの生成		
3.6.2 安全な暗号化キーの配布		
3.6.3 安全な暗号化キーの保存		
3.6.4 関連アプリケーション・ベンダーまたはキーオーナーが定義し、業界のベストプラクティスおよびガ		

イドライン（たとえば、NIST SP 800-57）に基づいた、暗号化期間の終了時点に到達したキーの暗号化キーの変更。暗号化期間の終了時点とは、たとえば、定義された期間が経過した後、または付与されたキーで一定量の暗号化テキストを作成した後（またはその両方）である。		
3.6.5 クリアテキスト・キーの知識を持つ従業員が離職したなど、キーの整合性が脆弱になっている場合、またはキーの脆弱性が悪用された可能性がある場合に必要な、キーの破棄または取り替え（アーカイブ、破壊、無効化など）。	Oracle MinClusterには、ZFSファイル・システム向けに保護され、一元化されたキー管理サービス（Solaris PKCS#11）があります。 また、キー管理業務に対応した、一元化されたOracle Walletもあります。オプションの一元キー管理ソリューションとしては、Oracle Key Management SystemやFIPS 140-2に準拠したオラクルのSun Crypto Accelerator 6000 PCIeカード（ハードウェア・セキュリティ・モジュール）などがサポートされています。	対応または適合

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

悪意のある個人が容易にアクセスできるネットワーク経由で機密情報を伝送する場合は、暗号化する必要があります。ワイヤレス・ネットワークの構成ミスや、古い暗号化プロトコルや認証プロトコルに潜む脆弱性は、こうした脆弱性につけこんでカード会員データ環境への特権アクセスを取得しようとする悪意のある個人の標的となり続けます。

Oracle MiniClusterでは、クライアント・ネットワーク、管理ネットワーク経由でIPSec、SSL/TLSおよびSSHを実装できます。オラクルの「デフォルトでのセキュリティ強化（SBD：secure-by-default）」により、デフォルト構成の場合はSSH以外でOracle MiniClusterにリモート・アクセスできないようになっており、管理トラフィックはすべて管理ネットワークに分離できるようになっています。

PCI要件	Oracle MiniClusterの詳細	適合または対応
4.1 オープンな公共ネットワーク経由で機密性の高いカード会員データを伝送する場合、以下を含む強力な暗号化とセキュリティ・プロトコルを使用する。 • 信頼できるキーと証明書のみを受け入れる。 • 使用されているプロトコルが、安全なバージョンまたは構成のみをサポートしている。 • 暗号化の強度が使用中の暗号化方式に適している。	Oracle MiniClusterはデフォルトで、クライアント・アクセスと管理アクセスが統合されたネットワーク上でコンポーネント間を伝送するカード会員データを、TLS/SSL、SSH、IPsecなどのテクノロジーを1つ以上使用して保護します。Oracle MiniClusterでは、すべてのネットワーク間のすべての伝送に対してIPSec、SSL/TLSの一方または両方を適用し、すべての管理インタフェースを保護できます。	適合

要件5：すべてのシステムをマルウェアから保護し、ウイルス対策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

ウイルス、ワーム、トロイの木馬など、一般に「マルウェア」と呼ばれる悪意のあるソフトウェアは、従業員の電子メールやインターネット、モバイル・コンピュータ、ストレージ・デバイスの使用をはじめとする多数の承認されたビジネスの活動中にネットワークに進入し、最終的にはシステムの脆弱性を悪用します。現行および新種の悪意のあるソフトウェアがもたらす脅威からシステムを保護するために、マルウェアに感染しやすいすべてのシステムでウイルス対策ソフトウェアを使用する必要があります。ウイルス対策ソフトウェアを補完するものとして、マルウェア対策ソリューションを追加することを検討してもよいでしょう。ただし、そのようなソリューションを追加しても、ウイルス対策ソフトウェアを導入する必要性がなくなるわけではありません。

Oracle MiniCluster（すなわちOracle Solaris）では、VSCANを通じて最大3つのサード・パーティ製ウイルス対策スキャナを使用して、ZFSファイル・システムのウイルス・スキャンを実施できます。

PCI要件	Oracle MiniClusterの詳細	適合または対応
5.1 悪意のあるソフトウェアの影響を受けやすいすべてのシステム（特にパーソナル・コンピュータとサーバー）に、ウイルス対策ソフトウェアを導入する。	VSCANを導入すれば、ZFSファイル・システムに保存されるコンテンツに対してリアルタイムでマルウェア対策スキャンを実施できます。 ウイルス・スキャンを実施するには、コンポーネントのVSCANサービスと既存の（外部の）ウイルス・スキャン・サービスを、業界標準プロトコルであるICAP（Internet Content Adaptation Protocol）を使用して統合します。	対応または適合
5.1.2 一般的に悪意のあるソフトウェアに影響されないとみなされているシステムでは、定期的に評価を行って、進化を続けるマルウェアの脅威を特定して評価することで、システムにウイルス対策ソフトウェアが依然として必要ないかどうかを判断する。		
5.2 すべてのウイルス対策メカニズムが以下のように維持されていることを確認する。 • 最新の状態である • 定期的にスキャンを行う • PCI DSS要件10.7に従って監査ログを作成・保持する。		

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

悪意を持った個人は、セキュリティの脆弱性を利用して、システムへの特権アクセスを手に入れます。このような脆弱性の多くは、ベンダー提供のセキュリティ・パッチにより修正できます。セキュリティ・パッチは、システムを管理する事業体がインストールする必要があります。悪意ある個人や悪意あるソフトウェアによるカード会員データの不正使用および侵害を阻止するため、すべてのシステムにすべての適切なソフトウェア・パッチをインストールする必要があります。

Oracle MiniClusterの重要な更新はオラクルのCritical Patch Updatesを通じて24時間365日いつでも入手できるため、ハードウェアとソフトウェアのライフサイクルを通じて脆弱性を確実に管理できます。Oracle MiniClusterでは、セキュアな分離テクノロジーと統合セキュリティ制御を利用することで、開発環境と本番環境を分離することができます。

PCI要件	Oracle MiniClusterの詳細	適合または対応
6.2 すべてのシステム・コンポーネントとソフトウェアに、ベンダー提供のセキュリティ・パッチがインストールされ、既知の脆弱性から保護されている。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。	Oracle MiniClusterは、オラクルのCritical Patch Updatesとセキュリティ・アラート（ライセンス契約を結んでいるユーザーは24時間365日いつでもセキュリティ更新やセキュリティ・パッチにアクセス可能）を利用することで、このPCI要件に適合するように容易に管理できます。Oracle MiniClusterの更新に関するニュースや通知はすべて、Oracle Critical Patch Update Advisoryを通じて顧客に提供されます。重要なセキュリティ更新は、すべてのコンポーネントとソフトウェア/ファームウェアで利用できます。 オラクルでは、Oracle Software Security Assurance（OSSA）という手法を採り入れ、すべてのOracle製品のセキュリティ開発ライフサイクルのあらゆる段階に情報セキュリティ管理のベスト・プラクティスを組み込み、リリースからサポート終了まで、ライフサイクルに従って継続的に脆弱性が管理されるようにしています。 適用されていないセキュリティ・パッチは、Oracle Enterprise Managerスイートで容易に検出できます。	対応
6.4.2 開発/テスト環境と本番環境での責務の分離	Oracle MiniClusterでは、セキュアな分離テクノロジーのほかに、通知と承認の機能が組み込まれた複数人による認証ワークフローを利用して、コンピュート、ネットワーク、ストレージおよびアプリケーションの各リソース領域において開発環境と本番環境が分離され、関連するアクセス制御システムが互いに独立するようにすることができます。	対応または適合

6.5.1 インジェクションの不具合（特にSQLインジェクション）。OSコマンド・インジェクション、LDAPおよびXPathのインジェクションの不具合、その他のインジェクションの不具合も考慮する。	Oracle Audit Vault and Database FirewallをOracle MiniClusterに追加すれば、データベースにアクセスするSQL文を高精度の次世代型SQL文法解析エンジンで検査し、データベースに影響が及ぶ前にSQLインジェクション攻撃を検出および阻止できます。Oracle Database Firewallは、アラート、ログ、置換、ホワイトリスト/ブラックリスト、SQLのブロック/許可を実行するよう構成でき、例外リスト制御が適用されます。これでこの要件が完全に満たされるわけではありませんが、適用される他のセキュリティ制御が強化され、これらの要件に対応する多重防御体制が整備されます。	対応
6.6 一般公開されているWebアプリケーションで、継続的に新たな脅威や脆弱性に対処し、これらのアプリケーションが、次のいずれかの方法によって既知の攻撃から保護されていることを確認する。 • 一般公開されているWebアプリケーションは、アプリケーションのセキュリティ脆弱性を手動/自動で評価するツールまたは手法によって、少なくとも年1回および何らかの変更を加えた後にレビューする。 注：この評価は、要件11.2で実施する脆弱性スキャンとは異なる。 • Webベースの攻撃を検知および回避するために、一般公開されているWebアプリケーションの手前に、自動化された技術ソリューション（Webアプリケーション・ファイアウォール）をインストールし、すべてのトラフィックを継続的にチェックする。		

COALFIRE

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

関係者のみが重要なデータにアクセスできるようにするために、職責に応じた必要な範囲にアクセスが制限されるようにシステムおよびプロセスを整備する必要があります。

「必要な範囲」とは、職務の遂行に必要な最小限のデータおよび権限に対してのみアクセス権が付与されることを指します。

Oracle MiniClusterでは、コンピュート、ストレージ、ネットワーク、アプリケーションのすべてのリソース領域でアクセス制御を細かく設定できます。

PCI要件	Oracle MiniClusterの詳細	適合または対応
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、業務上必要な個人に限定する。	Oracle MiniClusterのアクセス制御はいずれも、最小権限の原則を適用したRBAC（ロールベースのアクセス制御）を使用してあらかじめ構成されています。コンピュート、ネットワーク、ストレージ、アプリケーション、データベースの各レイヤーは、オラクルの細かな設定の可能なRBAC機能とPOSIXの権限を通じて、個々のサーバー、ストレージ、仮想化、オペレーティング・システムおよびデータベースのアクセス制御リストに変換されます。Oracle MiniClusterでは、ユーザーの必要性に基づいてアクセスを制限し、特に許可のない場合は「すべて拒否（deny all）」に設定されたアクセス制御システムを、オペレーティング・システム、データベースおよびアプリケーションのコンポーネントを対象にして確立することができます。	対応または適合
7.1.1 以下を含む、各役割のアクセスニーズを定義する。 • 各役割が職務上アクセスする必要のあるシステム・コンポーネントとデータリソース • リソースへのアクセスに必要な権限レベル（ユーザー、管理者など）		
7.1.2 特権ユーザーIDに与えるアクセス権を職務の実行に必要な最小限の特権に制限する。		
7.1.3 個人職種と職務に基づくアクセス権の割り当て。		
7.2 システム・コンポーネントで、ユーザーの必要性に基づいてアクセスが制限され、特に許可のない場合は「すべてを拒否」に設定された、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の項目を含める必要がある。		
7.2.1 すべてのシステム・コンポーネントを対象に含む。		
7.2.2 職種と職務に基づく、個人への特権の付与。		
7.2.3 デフォルトでは「すべてを拒否」の設定。		

COALFIRE

要件8：システム・コンポーネントに対するアクセスを識別して認証する

システム・コンポーネントにアクセスできる各ユーザーに一意の識別子（ID）を割り当てることで、各ユーザーが自分の行動に独自の責任を負うようにします。このような責任が課されている場合、重要なデータやシステムに対する操作が、既知の承認されているユーザーおよびプロセスによって実行されていることを確認できるだけでなく、追跡することもできます。

パスワードの有効性はおもに認証システムの設計と実装によって決まります。具体的には、攻撃者がパスワードを試行できる回数と、ユーザー・パスワードの入力時、送信時、保存時に保護するセキュリティ手法に左右されます

Oracle MiniClusterのデフォルト構成は、必要なすべてのユーザーに一意のIDが割り当てられ、ワークロード、ストレージ、ネットワーク、アプリケーション、データベースの各レイヤーへのアクセス権だけでなく、レイヤー間のアクセス権も認証できるようになっています。Oracle MiniClusterでは、Kerberosと監査機能、暗号化機能、ユーザー管理機能とを統合し、Kerberosに対応したアプリケーションを安全に保護することができます。Oracle Solarisの認証機能はプラグイン可能な認証モジュール（Pluggable Authentication Modules、PAM）を使用して柔軟に拡張できるため、Oracle MiniClusterにOracle Directory Server Enterprise EditionなどのLDAPディレクトリ・サービスまたはホストしている独立した任意のゾーンまたはすべてのゾーンに対する多要素認証（両方も可）を統合することができます。

PCI要件	Oracle MiniClusterの詳細	適合または対応
8.1.1 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、すべてのユーザーに一意のIDを割り当てる。	Oracle MiniClusterに適切なユーザーID管理セキュリティ・ポリシー構成を導入することで、これらの制御に準拠するように構成できます。 Oracle Identity ManagementなどのOracleスイート製品は、シングル・サインオン、Webベースのアクセス制御、Webサービス・セキュリティ、ID管理、強力な認証の他に、IDガバナンスとアクセス・ガバナンスにも対応できます。	対応または適合
8.1.2 ユーザーID、資格証明、その他の識別子オブジェクトの追加、削除、および変更を管理する。		
8.1.3 契約終了したユーザーのアクセスを直ちに取り消す。		
8.1.4 90日以内に非アクティブなユーザー・アカウントを削除/無効にする。		
8.1.5 第三者がリモート・アクセス経由でシステム・コンポーネントのアクセス、サポート、メンテナンスに使用するIDを以下のように管理する。 • 必要な期間内だけ有効になり、使用されていないときは無効になっている。 • 使用時だけ監視されている。		
8.1.6 6回以下の試行で、ユーザーIDをロックアウトすることによって、アクセスの試行回数を制限する。		
8.1.7 最低30分間、または管理者がユーザーIDを有効にするまでのロックアウト期間を設定する。		
8.1.8 セッションのアイドル状態が15分を超えた場合、ターミナルまたはセッションを再度アクティブにするため、ユーザーの再認証が必要となる。		

8.2 一意のIDを割り当てるだけでなく、すべてのユーザーを認証するため、次の方法の少なくとも1つを使用することで、すべてのシステム・コンポーネント上での顧客以外のユーザーと管理者の適切なユーザー認証管理を確認する。 • ユーザーが知っていること（パスワードやパスフレーズなど） • トークン・デバイスやスマート・カードなど、ユーザーが所有しているもの • ユーザー自身をしめすもの（生体認証など）	Oracle MiniClusterは、Radius、KerberosまたはSSL/TLSおよび、HMAC、OAuth2（事前統合済みのOracle Mobile Authenticatorモジュールを利用）またはGoogle Authenticatorモジュールを使用するワンタイム・パスワードを認証の手段として使用するように構成できます。	対応または適合
8.2.1 すべてのシステム・コンポーネントで強力な暗号化を使用して、送信と保存中に認証情報（パスワード/パスフレーズなど）をすべて読み取り不能としている。	Oracle MiniClusterでは、パスワードの保護、認証、保管時のデータ暗号化に次のアルゴリズムを利用しています。 • AES 128、192、256 • SHA-2 • RSA 2048、4096 Oracle MiniClusterのユーザー構成では、PCI DSSに対応するためのパスワード要件を容易に設定できます。さらに、オンデマンドのコンプライアンス・レポートにより、細かく設定されたパスワード要件を検証できます。	対応または適合
8.2.3 パスワード/パスフレーズは以下を満たす必要がある。 • パスワードに7文字以上が含まれる • 数字と英文字の両方を含む あるいは、上記のパラメータに等しい複雑さと強度を持つパスワード/パスフレーズ		
8.2.4 ユーザー・パスワード/パスフレーズは、少なくとも90日ごとに変更する。		
8.2.5 これまでに使用した最後の4つのパスワード/パスフレーズのいずれかと同じである新しいパスワード/パスフレーズを許可しない。		
8.2.6 初期パスワード/パスフレーズとリセットパスワード/パスフレーズをユーザーごとに一意の値にリセットし、初回の使用後直ちに変更する。		
8.3 すべてのコンソール以外の管理アクセスとCDEに対するすべてのリモート・アクセスを、多要素認証を使用してセキュリティで保護する。	Oracle MiniClusterは、2要素認証および、HMAC、OAuth2（事前統合済みのOracle Mobile Authenticatorモジュール）またはGoogle Authenticatorモジュールを使用するワンタイム・パスワードを認証の手段として使用するように事前に構成できます。	対応または適合
8.5.1 サービス・プロバイダ用の追加要件：（POSシステムやサーバーのサポートのために）顧客環境へのリモート・アクセス権を持つサービス・プロバイダは、各顧客環境に一意な認証情報（パスワード/パスフレーズなど）を使用する必要がある。	サービス・プロバイダは、各単一テナントをそれぞれが所有するカード会員データ環境に制限するようにOracle MiniClusterのアクセス制御を構成することで、この要件を確実に満たすことができます。アクセス制御は、RBACを使用して十分にきめ細かく行われるため、ホスティングされているどの事業体もそれぞれが所有するリソース以外にはアクセスできないように構成することができます。	対応または適合

8.6 他の認証メカニズムが使用されている場合（物理または論理セキュリティ・トークン、スマート・カード、証明書など）、そのメカニズムの使用は次のように割り当てられている。 • 認証メカニズムは、個々のアカウントに割り当てなければならず、複数アカウントで共有することはできない。 • 物理/論理制御により、意図されたアカウントのみがアクセスできるようにする必要がある。	Oracle MiniClusterはアクセス制御アーキテクチャにOracle SolarisのRBACを利用しています。Oracle MiniClusterは複数のロールをサポートしますが、これらのロールで実行されるすべてのアクションと操作は、ロール識別子ではなくユーザーIDに基づいてログに記録され監査されます。	対応または適合
8.7 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（アプリケーション、管理者、およびその他すべてのユーザーによるアクセスを含む）が以下のように制限されている。 • データベースへのユーザー・アクセス、データベースのユーザークエリ、データベースに対するユーザー・アクションはすべて、プログラムによる方法によってのみ行われる。 • データベースへの直接アクセスまたはクエリはデータベース管理者のみに制限される。 • データベース・アプリケーション用のアプリケーションIDを使用できるのはそのアプリケーションのみである（個々のユーザーやその他の非アプリケーション・プロセスは使用できない）。	Oracle MiniClusterは、企業向けの単一テナントまたは、クラウドにあるマルチテナント・システム内の専用コンピューティング環境として設計されています。最初のインストール時に、カード会員データを保管しているすべてのデータベースへのすべてのユーザー・アクセスに、細かな設定の可能なアクセス制御が実施されます。ユーザーには、この要件のすべての制御に適合するように権限を付与することができます。	対応または適合

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9には次のように記述されています。「カード会員データを収容するデータまたはシステムへの物理アクセスは、個人がデバイスやデータにアクセスして、システムやハードコピーを削除する機会を与えてしまうため、適切に制限する必要があります。要件9では、フルタイムおよびパートタイムの従業員、一時的な従業員、事業体の敷地内に"常駐"している請負業者やコンサルタントを"オンサイト要員"と呼び、ベンダー、オンサイト要員の来客、サービス業者など、施設に短期間（通常、1日以内）立ち入る必要のあるすべての人を"訪問者"と呼びます。また、カード会員データが含まれている紙媒体および電子媒体はすべて"媒体"とします。」

Oracle MiniCluster自体には、EEPROM（ブート・ローダー）のパスワードを設定する権限を管理者に付与する以外の物理的なセキュリティ制御はありませんが、コンピューティングとストレージの統合が可能で、クラウド・サービスが用意されていることにより、Oracle MiniClusterなどのエンジニアド・システムは、物理的なセキュリティ制御が強化されているデータセンターへの物理的な統合が可能だということになります。

COALFIRE

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

データ侵害の影響を阻止、検出、または最小化するために、ロギング・メカニズムとユーザー・アクティビティの追跡機能は重要です。すべての環境にログが存在することにより、何らかの不都合が起きても詳しい追跡、アラート通知、分析が実行できます。セキュリティ侵害の原因特定は、不可能ではないとしても、システム・アクティビティ・ログなしでは非常に困難です。

Oracle MiniClusterの統合監視/監査機能を使用すれば、データベースやアプリケーションに含まれるカード会員リソースへのアクセスを監視するよう規定したコンプライアンス要件を満たすことができます。そのため、単一テナント設計またはマルチテナント設計に対してPCI DSSが規定している多数の監視要件に準拠するよう、Oracle MiniClusterをコストやソフトウェア/ハードウェアの追加なしで構成することができます。

PCI要件	Oracle MiniClusterの詳細	適合または対応
10.1 システム・コンポーネントへのすべてのアクセスを各ユーザーにリンクする監査証跡を確立する。	Oracle MiniClusterの「監査ロール」に、すべての監査証跡の管理、審査、報告する権利および権限を定義できます。ロールはロール識別子ではなくユーザーIDに基づいて監査されるため、ユーザーが確実に識別され、管理者による重要データの誤用を防止できます。 Oracle Databaseでは細かな設定の可能な、条件付き監査ができるため、監査ログに含まれる不要な「ノイズ」の量を最小限に抑えながら、重要なユーザーと処理を確実に監査することができます。	対応または適合
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		
10.2.2 ルート権限または管理者権限を持つ個人によって行われたすべてのアクション		
10.2.3 すべての監査証跡へのアクセス		
10.2.4 無効な論理アクセス試行		
10.2.5 識別と認証メカニズムの使用および変更（新しいアカウントの作成、特権の昇格を含むがこれらに限定されない）、およびアカウントの変更、追加、削除のすべてはルートまたは管理者権限が必要である。		
10.2.6 監査ログの初期化、停止、一次停止		
10.2.7 システムレベル・オブジェクトの作成および削除		
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 ユーザー識別子		
10.3.2 イベントの種類		
10.3.3 日付と時刻		
10.3.4 成功または失敗を示す情報		
10.3.5 イベントの発生元		
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		

10.4 時刻同期技術を使用してすべての重要なシステム・クロックおよび時間を同期し、時間を取得、配布、保存するために以下の要件が実施されていることを確認する。	Oracle MiniClusterでは、Network Time Protocol（NTP）サービスを利用してプラットフォーム全体の時刻を同期させます。NTPサービスをOracle MiniClusterの監視/監査機能と組み合わせることで、この要件に準拠するように構成できます。	対応
10.4.1 重要なシステムが正確で一貫性のある時刻を持っている。		
10.4.2 時刻データが保護されている。		
10.4.3 時刻設定は、業界で認知されている時刻ソースから受信されている。		
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。	Oracle MiniClusterのストレージへのアクセスは、ユーザーとロールに基づくアクセス制御をはじめとするさまざまな認証手法とアクセス制御技術で制御されています。また、データベースとファイル・システムのストレージを暗号化することで、保管中のデータへの不正なアクセスをさらに厳しく防止できます。さらに、必要な場合は、Oracle SolarisとOracle Databaseの監査データを外部のストレージや処理機能にオフロードできます。	対応または適合
10.5.1 仕事関連のニーズを持つ個人に監査証跡の表示を制限する。	この管理項目に適合させるために、Oracle MiniClusterはRBACと最小権限モデルを使用してあらかじめ構成されており、必要最小限の権限が付与されたロールを持つユーザーのみにログへのアクセスを許可するロールベースのアクセス制御が適用されています。なお、これはOracle SolarisとOracle Databaseの両方の監査証跡に該当します。	適合
10.7 監査証跡の履歴を少なくとも1年間保持し、少なくとも3カ月間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）。	Oracle MiniClusterの一元化された監視機能とログ管理機能は、この管理項目の遵守に必要な保存期間要件が満たされるようにインストール時に事前構成されます。	適合

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

脆弱性は、悪意のある個人や研究者によって絶えず発見され、新しいソフトウェアによって絶えず生じています。変化を続ける環境にセキュリティ制御を絶えず確実に反映させるには、システム・コンポーネント、プロセス、カスタム・ソフトウェアを頻繁にテストする必要があります。

Oracle MiniClusterにIDS/IPSシステムや変更検出機能は事前構成されていませんが、IDS/IPSセンサーを統合するか、サード・パーティ製のホストベースのソリューションを利用することで、Oracle MiniClusterの上流の着信および発信トラフィックを監視することができます。変更検出機能を補い管理項目に適合するために、Oracle MiniClusterではカスタムのファイル変更監視機能として、基本監査報告機能（BART）、ベリファイド・ブート、強固なアクセス制御も利用できます。

要件12：すべての担当者の情報セキュリティ・ポリシーを整備する

厳しいセキュリティ・ポリシーは事業体全体のセキュリティ意識を決めるものであり、担当者に期待されていることは何かを伝えるものでもあります。データの機密性とそれを保護する責任を、すべての担当者が認識する必要があります。要件12では、フルタイムおよびパートタイムの従業員、一時的な従業員、事業体の敷地内に「常駐」しているか、またはカード会員データ環境にアクセスできる請負業者やコンサルタントを「担当者」と呼びます。

PCI DSS v3.2の要件12全体で詳述されている各要件は、PCI DSSのすべての要件とベスト・プラクティスの技術的な管理項目とプロセス面での管理項目を実施するのに必要なポリシーと手続きを対象にしているため、この要件に含まれる管理項目のうちOracle MiniClusterで適合または対応できるものはありません。

PCI DSS付録A：共有ホスティング・プロバイダ向けのPCI DSS追加要件

要件 A.1：共有ホスティング・プロバイダは、カード会員データ環境を保護すること

要件12.8および12.9の記述のとおり、カード会員データにアクセスするすべてのサービス・プロバイダ（共有ホスティング・プロバイダを含む）は、PCI DSSを遵守しなければなりません。さらに、要件2.6には、共有ホスティング・プロバイダはそれぞれの事業体のホスト環境やデータを保護しなければならない、と記載されています。したがって、共有ホスティング・プロバイダは、この付録の要件についても遵守しなければなりません。

Oracle MiniClusterは単一テナント環境の提供を目的としていますが、Oracle MiniCluster仮想マシンを使用してホスト・アプリケーションを論理的に分離し、仮想マシンのサンドボックス機能を利用して隔離を実現できるため、マルチテナント・サービス・プロバイダのITコンプライアンス・ポリシーに適合します。また、専用コンピューティング環境としてセキュアに分離し、厳密にアクセス制御することで、「共有ホスティング・プロバイダ向けのPCI DSS要件」に適合するようにOracle MiniClusterを構成することができます。

PCI要件	Oracle MiniClusterの詳細	適合または対応
A1.1 各事業体が、その事業体のカード会員データ環境にアクセスするプロセスのみを実行するようにする。	Oracle MiniClusterは、単一テナントのセキュアなコンピューティング環境として使用されることを想定しています。	対応または適合
A1.2 各事業体のアクセスおよび特権が、その事業体のカード会員データ環境のみに制限されている。	Oracle MiniClusterの細かな設定が可能なアクセス制御は、ホストされているどの事業体も、その事業体が所有するリソースへのアクセスのみ許可されるよう、インストール時に事前構成されます。専用コンピューティング・プラットフォームであるOracle MiniClusterでは、ユーザー、グループ、ロール、認証メカニズム、ロギングおよび監査証跡の独立した専用のセットが、必要な個々のテナントに割り当てられるようになっています。	適合

A1.3 ログ記録と監査証跡が有効になっていて、各事業体のカード会員データ環境に一意であり、PCI DSS要件10と一致していることを確認する。	Oracle MiniClusterの監視機能は、要件10に準拠するようあらかじめテナントごとに構成されています。アプリケーション、データベース、ネットワーク、およびカード会員データへのアクセスの監視は、ログの集約やSIEMによる分析を可能にするために、syslog機能を活用するように構成することができます。	適合
A1.4 ホストされている加盟店またはサービス・プロバイダへの侵害が発生した場合に、タイムリーなフォレンジック調査を提供するプロセスを可能にする。	Oracle MiniClusterは、監視、細かな設定が可能な監査とロギング、ウイルス・スキャン（VSCAN）を通じてこの要件に対応するように構成できます。さらに、データベースやアプリケーション固有の制御を行えば、管理操作やユーザー・アクティビティやその他のデータをさらに詳しく調査および記録できます。	対応

有効なPCI管理項目とSOC2の対応表

Oracle MiniClusterは、PCIの要件に適合または対応するだけでなく、SOC2 Trustサービス基準に取り組んでいる組織を支援できる機能も多数搭載しています。これを示すために、Oracle MiniClusterが適合または対応しているPCI 3.2の要件と、同時に対応すると考えられるSOC2の基準とを関連付けました（下記の表を参照）。なお、SOC2の基準に適合させるために、Oracle MiniClusterの使用について独自の管理項目を規定する責任は、依然として残ります。SOC2 Trustサービス基準の内容は付録Aを参照してください。

PCI要件	Oracle MiniClusterの詳細	適合または対応	対応するSOC2の基準
1.2 信頼できないネットワークとカード会員データ環境内のすべてのシステム・コンポーネントの接続を制限する、ファイアウォールとルーターの構成を構築する。	Oracle MiniClusterでは、Solarisの IPフィルタを介したホストベースのファイアウォール・パケット・フィルタリングにより、公開されているサービスへのネットワーク・アクセスを制限できます。IPフィルタは、仮想マシン・レベルまたはアクセス制御リスト（または両方）で着信および発信ネットワーク・トラフィックのポリシーを適用し、物理デバイスと仮想デバイスとの間の通信を制限できます。	対応	CC5.6
1.2.1 着信および発信トラフィックを、カード会員データ環境に必要なトラフィックにし、それ以外のすべてのトラフィックを特定的に拒否する。	Oracle SolarisのIPフィルタが、着信および発信トラフィックを必要なトラフィックのみに制限するようあらかじめ構成されており、デフォルトは、導入されている仮想マシン上のトラフィックをすべて拒否（deny-all）するように構成されています。	対応または適合	CC5.6

PCI要件	Oracle MiniClusterの詳細	適合または対応	サポートされるSOC2の基準
1.2.3 すべてのワイヤレス・ネットワークとカード会員データ環境の間に境界ファイアウォールをインストールし、ワイヤレス環境とカード会員データ環境間のトラフィックを拒否または、業務上必要な場合、承認されたトラフィックのみを許可するようにファイアウォールを構成する。	Oracle SolarisのIPフィルタをステートフル・パケット・インスペクション・ファイアウォールとして利用すると、Oracle MiniCluster外のすべてのワイヤレス・ネットワークとOracle MiniCluster上のすべてのカード会員データ環境ネットワークをファイアウォールで分離できます。アクセスが必要な場合は、Oracle MiniClusterのステートフル・ファイアウォールで、どのネットワーク・ベースのステートフル・パケット・インスペクション・ファイアウォールとも同じように非常にきめ細かくカード会員データ環境へのアクセスを設定できます。	対応	CC5.6
1.3 インターネットとカード会員データ環境内のすべてのシステム・コンポーネント間の、直接的なパブリック・アクセスを禁止する。	Oracle SolarisのIPフィルタをネットワーク・ベースのファイアウォールまたは境界ルーターのファイアウォール機能およびアクセス制御リストと組み合わせることで、カード会員データ環境との間の直接的なアクセスをすべて禁止することができます。	対応	CC5.6
1.3.4 カード会員データ環境からインターネットへの不正な発信トラフィックを禁止する。	Oracle MiniClusterのホストベースのIPフィルタ・ステートフル・パケット・インスペクション・ファイアウォールが、認可されたトラフィックのみカード会員データ環境からインターネットに発信されるように、出口アクセス制御リストを使用してあらかじめ構成されています。	適合	CC5.6
1.3.5 ネットワーク内へは、「確立された」接続のみを許可する。	Oracle MiniClusterのIPフィルタ・ステートフル・パケット・インスペクション・ファイアウォールが、この要件に適合するようにあらかじめ構成されています。イーサネットを介したステートフル・パケット・フィルタリングがサポートされています。	適合	CC5.6
1.3.6 DMZやその他の信頼できないネットワークから隔離されている内部ネットワーク・ゾーンで、カード会員データを保存するコンポーネント（データベース）が実装されている。	Oracle MiniClusterのIPフィルタ・ステートフル・パケット・インスペクション・ファイアウォールが、この要件に適合するようにあらかじめ構成されています。	適合	CC5.6

PCI要件	Oracle MiniClusterの詳細	適合または対応	サポートされるSOC2の基準
1.3.7 プライベートIPアドレスとルーティング情報を許可されていない第三者に開示しない。 注：IPアドレスを開示しない方法には、以下のものが含まれるが、これに限定されるわけではない： • ネットワーク・アドレス変換（NAT） • カード会員データを保持するサーバーをプロキシサーバー/ファイアウォールの背後に配置する。 • 登録されたアドレス指定を使用するプライベート・ネットワークのルート・アドバタイズを削除するか、フィルタリングする。 • 登録されたアドレスの代わりにRFC1918アドレス空間を内部で使用する。	権限を持たない第三者にプライベートIPアドレスやルーティング情報が開示されないようにするために、ネットワーク・アドレス変換とポート・アドレス変換を実行するよう、Oracle MiniClusterのIPフィルタがあらかじめ構成されています。	適合	CC5.6
1.4 インターネットに直接接続するポータブル・コンピューテ・デバイス（会社あるいは従業員が所有するものも含む）で、ネットワークの外側ではインターネットに接続され、またCDEへのアクセスにも使用されるものに（従業員が使用するラップトップなど）、パーソナル・ファイアウォール・ソフトウェアか同等機能のソフトウェアをインストールする。ファイアウォール（またはそれに相当する）構成には以下が含まれます。 • 特定の構成設定が定義されている。 • パーソナル・ファイアウォール（またはそれに相当する機能）がアクティブに実行中である。 • パーソナル・ファイアウォール（またはそれに相当する機能）がモバイル・デバイスのユーザーによって変更できないようになっている。	ホストされている仮想ゲスト・コンピュータには、Oracle SolarisのIPフィルタ・ファイアウォールがホストベースのファイアウォールとしてあらかじめインストールされています。事前定義された固有の構成設定一式はあらかじめ構成されており、ファイアウォールは常時稼働し、ユーザーはファイアウォールの構成を変更できないようになっています。	適合	CC5.6

PCI要件	Oracle MiniClusterの詳細	適合または対応	サポートされるSOC2の基準
2.1 システムをネットワーク上に導入する前に、必ずベンダー提供のデフォルト値を変更し、不要なデフォルト・アカウントを無効にする。 これは、オペレーティング・システム、セキュリティ・サービスを提供するソフトウェア、アプリケーション、システム・アカウント、POS端末、ペイメント・アプリケーション、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で使用されるが、これらに限定されない、すべてのデフォルト・パスワードに適用されます。	Oracle MiniClusterに組み込まれている一部のオラクル製品は、デフォルトの管理パスワードを設定した状態で納品されるため、使用する前に変更する必要があります。セキュリティ・ガイドを参考にして、組織の構成基準に合わせて構成をカスタマイズしてください。 Oracle MiniClusterをインストールすると、ほとんどのネットワーク・サービスは「デフォルトでのセキュリティ強化」機能によって無効化され、SSH以外ではリモート・アクセスができなくなります。	対応または適合	CC5.6
2.2.1 同じサーバーに異なったセキュリティ・レベルを必要とする機能が共存しないように、1つのサーバーには、主要機能を1つだけ実装する。（たとえば、Webサーバー、データベース・サーバー、DNSは別々のサーバーに実装する必要がある）。	オラクルの仮想化テクノロジーを使用すると、1つの主要機能だけを提供する仮想ホストを作成することができます。 Oracle MiniClusterのコンプライアンス・レポート機能は、ベンチマークをテストしてコンプライアンスの成否を示す報告書を作成する機能です。	対応または適合	CC5.6
2.2.2 システムの機能に必要なサービス、プロトコル、デーモンなどのみを有効にする。	Oracle Solarisには「デフォルトでのセキュリティ強化」機能があるため、不要なサービス、プロトコル、デーモン/サーバーは決して実行されず、SSH以外のプロトコルではリモート接続のリッスンは行われず、ローカル・アクセス以外は権限を昇格することができません。	対応または適合	CC5.6
2.2.3 安全でないとみなされている必要なサービス、プロトコル、またはデーモンに追加のセキュリティ機能を実装する。	Oracle MiniClusterはデフォルトでセキュアなサービスのみを利用するため、Oracle MiniClusterをデフォルト構成で使用する場合はセキュリティ機能を追加する必要はありません。セキュアでないサービス、プロトコル、またはデーモン（サーバー）のセキュリティを強化するために防御層を追加する場合は、この要件に適合または対応するためにPCI-DSSセキュリティ・プロファイルをインストール時に選択することで、アクセス制御、ステートフル・パケット・インスペクション、セキュア・ゾーンの隔離、強力な認証およびロギングを事前構成することができます。	適合	CC5.6

PCI要件	Oracle MiniClusterの詳細	適合または対応	サポートされるSOC2の基準
2.2.5 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、および不要なWebサーバーなど、すべての不要な機能を削除する。	攻撃の対象となる範囲を狭めるOracle MiniClusterの「デフォルトでのセキュリティ強化」機能により、多数のネットワーク・サービスをひとまとめにした形で不要な機能を無効化し、ローカル以外ではアクセス権を高くすることができないようにしています。また、着信ネットワーク接続はSSHでのみ可能です。Oracle Solarisには、デフォルトで接続をリッスンするWebサーバーがありません。	適合	CC5.6
2.3 強力な暗号化を使用して、すべてのコンソール以外の管理アクセスを暗号化する。	Oracle MiniCluster Virtual AssistantはTLS 1.2またはSSHを使用して機密情報の漏洩や管理用接続の乗っ取りを防止します。	対応または適合	CC5.7
2.6 共有ホスティング・プロバイダは、各事業体のホスト環境およびカード会員データを保護する必要がある。これらのプロバイダは、付録A1：「共有ホスティング・プロバイダでの追加PCI DSS要件」に示されているように、特定の要件を満たす必要がある。	Oracle MiniClusterの統合監視、アクセス制御、および暗号化は、セキュアな分離テクノロジーと組み合わせることで、付録A：「共有ホスティング・プロバイダ向けのPCI DSS追加要件」を確実に遵守するように設計および構成できます。	対応	なし
3.2 承認後に機密認証データを保存しない（暗号化されている場合でも）。機密認証データを受け取った場合、認証プロセスが完了し次第すべてのデータを復元不能にする。以下の場合に、データが安全に保存される場合は、発行者と企業が、機密認証データを保存するため、発行サービスをサポートすることが可能である。 • 業務上の理由がある • データが安全に保存されている	PCI DSSは機密認証データの保存を厳格に禁止していますが、業務上の正当な理由があって保存する必要がある場合や、組織が発行者であったり発行業務をサポートしていたりすることから保存する必要がある場合がまれにあります。業務上の正当な理由があって機密認証データを保存しなければならない場合は、Oracle MiniClusterを利用すればすべての機密情報が暗号化されます。Oracle MiniClusterでは、データベース表領域の透過的データ暗号化（TDE）か、ファイル・システムのセキュリティを確保するデフォルトのZFSベースのディスク暗号化の一方または両方を使用できます。	対応または適合	なし

PCI要件	Oracle MiniClusterの詳細	適合または対応	サポートされるSOC2の基準
3.4 以下の手法を使用して、すべての場所で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、ログのデータを含む）。 • 強力な暗号化をベースにしたワンウェイ・ハッシュ（PAN全体をハッシュする必要がある） • トランケーション（PANの切り捨てられたセグメントの置き換えにはハッシュを使用できない） • 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	Oracle MiniClusterでは、データベース内のデータをTDEで暗号化（ファイルレベルまたは列レベルのデータベース暗号化）する場合や、保管されているデータにZFSディスク暗号化を適用する場合に、複数の暗号化アルゴリズムと鍵の強度を利用できます。TDEもZFS暗号化も、この項目の制御に準拠する方法で実装できます。 Oracle Databaseを利用して、データ全体またはデータのほんの一部が固定値またはマスク値で置き換えられるようにすることができます。	適合	なし
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・システムの認証および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・データベースや一般的なネットワーク・ログイン資格情報を使用しないなどの方法で）。復号キーがユーザー・アカウントと関連付けられていない。	ZFS暗号化は、ユーザー・アカウントと関連付けられない方法でディスク暗号化が実装されるように、最初のインストール時に事前構成されます。Oracle MiniClusterには、「Oracle Key Manager」をネットワークHSMアプライアンスとして使用して暗号化アクセラレーションのシームレスな提供や暗号化キー管理機能のオフロードを可能にする構成の統合を支援する機能があります。また、複数のサード・パーティ製HSM製品と統合して、暗号化キー管理機能をオフロードしたり暗号化アクセラレーションを提供したりすることもできます。	適合	なし

PCI要件	Oracle MiniClusterの詳細	適合または対応	サポートされるSOC2の基準
3.5.3 カード会員データの暗号化/復号化に使用される秘密キーは、以下のいずれかの形式（複数可）で常時保存する。 • 少なくともデータ暗号化キーと同じ強度のキー暗号化で暗号化されており、データ暗号化キーとは別の場所に保管されている • 安全な暗号化デバイス（ホスト・セキュリティ・モジュール（HSM）またはPTS承認の加盟店端末装置など） • 業界承認の方式に従う、少なくとも2つの全長キーコンポーネントまたはキー共有として	Oracle MiniClusterには、ZFS暗号化キー、データベース固有のキーやアプリケーション固有のキーを保存するための、PKCS#11ベースの一元化されたキーストアがあらかじめ構成されています。また、PKCS#11またはKMIPのインタフェースを使用するHSMへの移行準備を支援する機能があります。	対応または適合	なし
3.5.4 暗号化キーを最小限の場所に保存する。			
3.6.1 強力な暗号化キーの生成			
3.6.2 安全な暗号化キーの配布			
3.6.3 安全な暗号化キーの保存			
3.6.4 関連アプリケーション・ベンダーまたはキーオーナーが定義し、業界のベストプラクティスおよびガイドライン（たとえば、NIST SP 800-57）に基づいた、暗号化期間の終了時点に到達したキーの暗号化キーの変更。暗号化期間の終了時点とは、たとえば、定義された期間が経過した後、または付与されたキーで一定量の暗号化テキストを作成した後（またはその両方）である。			

PCI要件	Oracle MiniClusterの詳細	適合または対応	サポートされるSOC2の基準
3.6.5 クリアテキスト・キーの知識を持つ従業員が離職したなど、キーの整合性が脆弱になっている場合、またはキーの脆弱性が悪用された可能性がある場合に必要な、キーの破棄または取り替え（アーカイブ、破壊、無効化など）。	Oracle MinClusterには、ZFSファイル・システム向けに保護され、一元化されたキー管理サービス（Solaris PKCS#11）があります。 また、キー管理業務に対応した、一元化されたOracle Walletもあります。オプションの一元キー管理ソリューションとしては、Oracle Key Management SystemやFIPS 140-2に準拠したオラクルのSun Crypto Accelerator 6000 PCIeカード（ハードウェア・セキュリティ・モジュール）などがサポートされています。	対応または適合	なし
4.1 オープンな公共ネットワーク経由で機密性の高いカード会員データを伝送する場合、以下を含む強力な暗号化とセキュリティ・プロトコルを使用する。 • 信頼できるキーと証明書のみを受け入れる。 • 使用されているプロトコルが、安全なバージョンまたは構成のみをサポートしている。 • 暗号化の強度が使用中の暗号化方式に適している。	Oracle MiniClusterはデフォルトで、クライアント・アクセスと管理アクセスが統合されたネットワーク上でコンポーネント間を伝送するカード会員データを、TLS/SSL、SSH、IPsecなどのテクノロジーを1つ以上使用して保護します。Oracle MiniClusterでは、すべてのネットワーク間のすべての伝送に対してIPSec、SSL/TLSの一方または両方を適用し、すべての管理インタフェースを保護できます。	適合	CC5.7
5.1 悪意のあるソフトウェアの影響をうけやすいすべてのシステム（特にパーソナル・コンピュータとサーバー）に、ウイルス対策ソフトウェアを導入する。 5.1.2 一般に悪意のあるソフトウェアに影響されないとみなされているシステムでは、定期的に評価を行って、進化を続けるマルウェアの脅威を特定して評価することで、システムにウイルス対策ソフトウェアが依然として必要ないかどうかを判断する。 5.2 すべてのウイルス対策メカニズムが以下のように維持されていることを確認する。 • 最新の状態である • 定期的にスキャンを行う • PCI DSS要件10.7に従って監査ログを生成・保持する。	VSCANを導入すれば、ZFSファイル・システムに保存されるコンテンツに対してリアルタイムでマルウェア対策スキャンを実施できます。 ウイルス・スキャンを実施するには、コンポーネントのVSCANサービスと既存の（外部の）ウイルス・スキャン・サービスを、業界標準プロトコルであるICAP（Internet Content Adaptation Protocol）を使用して統合します。	対応または適合	CC5.8

PCI要件	Oracle MiniClusterの詳細	適合または対応	サポートされるSOC2の基準
6.2 すべてのシステム・コンポーネントとソフトウェアに、ベンダー提供のセキュリティ・パッチがインストールされ、既知の脆弱性から保護されている。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。	Oracle MiniClusterは、オラクルのCritical Patch Updatesとセキュリティ・アラート（ライセンス契約を結んでいるユーザーは24時間365日いつでもセキュリティ更新やセキュリティ・パッチにアクセス可能）を利用することで、このPCI要件に適合するように容易に管理できます。Oracle MiniClusterの更新に関するニュースや通知はすべて、Oracle Critical Patch Update Advisoryを通じて顧客に提供されます。重要なセキュリティ更新は、すべてのコンポーネントとソフトウェア/ファームウェアで利用できます。 オラクルでは、Oracle Software Security Assurance（OSSA）という手法を採り入れ、すべてのOracle製品のセキュリティ開発ライフサイクルのあらゆる段階に情報セキュリティ管理のベスト・プラクティスを組み込み、リリースからサポート終了まで、ライフサイクルに従って継続的に脆弱性が管理されるようにしています。 適用されていないセキュリティ・パッチは、Oracle Enterprise Managerスイートで容易に検出できます。	対応	CC5.1、CC5.6、CC5.8
6.4.2 開発/テスト環境と本番環境での責務の分離	Oracle MiniClusterでは、セキュアな分離テクノロジーのほかに、通知と承認の機能が組み込まれた複数人による認証ワークフローを利用して、コンピュート、ネットワーク、ストレージおよびアプリケーションの各リソース領域において開発環境と本番環境が分離され、関連するアクセス制御システムが互いに独立するようにすることができます。	対応または適合	CC7.4

PCI要件	Oracle MiniClusterの詳細	適合または対応	サポートされるSOC2の基準
6.5.1 インジェクションの不具合（特にSQLインジェクション）。OSコマンド・インジェクション、LDAPおよびXPathのインジェクションの不具合、その他のインジェクションの不具合も考慮する。 6.6 一般公開されているWebアプリケーションで、継続的に新たな脅威や脆弱性に対処し、これらのアプリケーションが、次のいずれかの方法によって、既知の攻撃から保護されていることを確認する。 • 一般公開されているWebアプリケーションは、アプリケーションのセキュリティ脆弱性を手動/自動で評価するツールまたは手法によって、少なくとも年1回および何らかの変更を加えた後にレビューする。 注：この評価は、要件11.2で実施する脆弱性スキャンとは異なる。 • Webベースの攻撃を検知および回避するために、一般公開されているWebアプリケーションの手前に、自動化された技術ソリューション（Webアプリケーション・ファイアウォール）をインストールし、すべてのトラフィックを継続的にチェックする。	Oracle Audit Vault and Database FirewallをOracle MiniClusterに追加すれば、データベースにアクセスするSQL文を高精度の次世代型SQL文法解析エンジンで検査し、データベースに影響が及ぶ前にSQLインジェクション攻撃を検出および阻止できます。Oracle Database Firewallは、アラート、ログ、置換、ホワイトリスト/ブラックリスト、SQLのブロック/許可を実行するよう構成でき、例外リスト制御が適用されます。これでこの要件が完全に満たされるわけではありませんが、適用される他のセキュリティ制御が強化され、これらの要件に対応する多重防御体制が整備されます。	対応	なし

PCI要件	Oracle MiniClusterの詳細	適合または対応	サポートされるSOC2の基準
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、業務上必要な個人に限定する。	Oracle MiniClusterのアクセス制御はいずれも、最小権限の原則を適用したRBAC（ロールベースのアクセス制御）を使用してあらかじめ構成されています。コンピュート、ネットワーク、ストレージ、アプリケーション、データベースの各レイヤーは、オラクルの細かな設定の可能なRBAC機能とPOSIXの権限を通じて、個々のサーバー、ストレージ、仮想化、オペレーティング・システムおよびデータベースのアクセス制御リストに変換されます。Oracle MiniClusterでは、ユーザーの必要性に基づいてアクセスを制限し、特に許可のない場合は「すべて拒否（deny-all）」に設定されたアクセス制御システムを、オペレーティング・システム、データベースおよびアプリケーションのコンポーネントを対象にして確立することができます。	対応または適合	CC5.1、CC5.4
7.1.1 以下を含む、各役割のアクセスニーズを定義する。 • 各役割が職務上アクセスする必要のあるシステム・コンポーネントとデータリソース • リソースへのアクセスに必要な権限レベル（ユーザー、管理者など）			
7.1.2 特権ユーザーIDに与えるアクセス権を職務の実行に必要な最小限の特権に制限する。			
7.1.3 個人職種と職務に基づくアクセス権の割り当て。			
7.2 システム・コンポーネントで、ユーザーの必要性に基づいてアクセスが制限され、特に許可のない場合は「すべてを拒否」に設定された、アクセス制御システム確立する。 アクセス制御システムには以下の項目を含める必要がある。			
7.2.1 すべてのシステム・コンポーネントを対象に含む。			
7.2.2 職種と職務に基づく、個人への特権の付与。			
7.2.3 デフォルトでは「すべてを拒否」の設定。			

PCI要件	Oracle MiniClusterの詳細	適合または対応	サポートされるSOC2の基準
8.1.1 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、すべてのユーザーに一意のIDを割り当てる。	Oracle MiniClusterに適切なユーザーID管理セキュリティ・ポリシー構成を導入することで、これらの制御に準拠するように構成できます。 Oracle Identity ManagementなどのOracleスイート製品は、シングル・サインオン、Webベースのアクセス制御、Webサービス・セキュリティ、ID管理、強力な認証の他に、IDガバナンスとアクセス・ガバナンスにも対応できます。	対応または適合	CC5.1、CC5.3
8.1.2 ユーザーID、資格証明、その他の識別子オブジェクトの追加、削除、および変更を管理する。			
8.1.3 契約終了したユーザーのアクセスをただちに取り消す。			
8.1.4 90日以内に非アクティブなユーザー・アカウントを削除/無効にする。			
8.1.5 第三者がリモート・アクセス経由でシステム・コンポーネントのアクセス、サポート、メンテナンスに使用するIDを以下のように管理する。 • 必要な期間内だけ有効になり、使用されていないときは無効になっている。 • 使用時だけ監視されている。			
8.1.6 6回以下の試行で、ユーザーIDをロックアウトすることによって、アクセスの試行回数を制限する。			
8.1.7 最低30分間、または管理者がユーザーIDを有効にするまでのロックアウト期間を設定する。			
8.1.8 セッションのアイドル状態が15分を超えた場合、ターミナルまたはセッションを再度アクティブにするため、ユーザーの再認証が必要となる。			

PCI要件	Oracle MiniClusterの詳細	適合または対応	サポートされるSOC2の基準
8.2 一意のIDを割り当てることに加え、すべてのユーザーを認証するため、次の方法の少なくとも1つを使用することで、すべてのシステム・コンポーネント上での顧客以外のユーザーと管理者の適切なユーザー認証管理を確認する。 • ユーザーが知っていること（パスワードやパスフレーズなど） • トークン・デバイスやスマート・カードなど、ユーザーが所有しているもの • ユーザー自身を示すもの（生体認証など）	Oracle MiniClusterは、Radius、KerberosまたはSSL/TLSおよび、HMAC、OAuth2（事前統合済みのOracle Mobile Authenticatorモジュールを利用）またはGoogle Authenticatorモジュールを使用するワンタイム・パスワードを認証の手段として使用するように構成できます。	対応または適合	なし
8.2.1 すべてのシステム・コンポーネントで強力な暗号化を使用して、送信と保存中に認証情報（パスワード/パスフレーズなど）をすべて読み取り不能としている。	Oracle MiniClusterでは、パスワードの保護、認証、保管時のデータ暗号化に次のアルゴリズムを利用しています。 • AES 128、192、256 • SHA-2 • RSA 2048、4096 Oracle MiniClusterのユーザー構成では、PCI DSSに対応するためのパスワード要件を容易に設定できます。 さらに、オンデマンドのコンプライアンス・レポートにより、細かく設定されたパスワード要件を検証できます。	対応または適合	CC5.1、CC5.3
8.2.3 パスワード/パスフレーズは以下を満たす必要がある。 • パスワードに7文字以上が含まれる • 数字と英文字の両方を含む あるいは、上記のパラメータに等しい複雑さと強度を持つパスワード/パスフレーズ			
8.2.4 ユーザー・パスワード/パスフレーズは、少なくとも90日ごとに変更する。			
8.2.5 これまでに使用した最後の4つのパスワード/パスフレーズのいずれかと同じである新しいパスワード/パスフレーズを許可しない。			
8.2.6 初期パスワード/パスフレーズとリセットパスワード/パスフレーズをユーザーごとに一意の値にリセットし、初回の使用後直ちに変更する。			

PCI要件	Oracle MiniClusterの詳細	適合または対応	サポートされるSOC2の基準
8.3 すべてのコンソール以外の管理アクセスとCDEに対するすべてのリモート・アクセスを、多要素認証を使用してセキュリティで保護する。	Oracle MiniClusterは、2要素認証および、HMAC、OAuth2（事前統合済みのOracle Mobile Authenticatorモジュール）またはGoogle Authenticatorモジュールを使用するワンタイム・パスワードを認証の手段として使用するように事前に構成できます。	対応または適合	CC5.1
8.5.1 サービス・プロバイダ用の追加要件：（POSシステムやサーバーのサポートのために）顧客環境へのリモート・アクセス権を持つサービス・プロバイダは、各顧客環境に一意な認証情報（パスワード/パスフレーズなど）を使用する必要がある。	サービス・プロバイダは、各単一テナントをそれぞれが所有するカード会員データ環境に制限するようにOracle MiniClusterのアクセス制御を構成することで、この要件を確実に満たすことができます。アクセス制御は、RBACを使用して十分にきめ細かく行われるため、ホスティングされているどの事業体もそれぞれが所有するリソース以外にはアクセスできないように構成することができます。	対応または適合	CC5.1
8.6 他の認証メカニズムが使用されている場合（物理または論理セキュリティ・トークン、スマート・カード、証明書など）、そのメカニズムの使用は次のように割り当てられている。 • 認証メカニズムは、個々のアカウントに割り当てなければならず、複数アカウントで共有することはできない。 • 物理/論理制御により、意図されたアカウントのみがアクセスできるようにする必要がある。	Oracle MiniClusterはアクセス制御アーキテクチャにOracle SolarisのRBACを利用しています。Oracle MiniClusterは複数のロールをサポートしますが、これらのロールで実行されるすべてのアクションと操作は、ロール識別子ではなくユーザーIDに基づいてログに記録され監査されます。	対応または適合	CC5.1、CC5.3

PCI要件	Oracle MiniClusterの詳細	適合または対応	サポートされるSOC2の基準
8.7 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（アプリケーション、管理者、およびその他すべてのユーザーによるアクセスを含む）が以下のように制限されている。 • データベースへのユーザー・アクセス、データベースのユーザークエリ、データベースに対するユーザー・アクションはすべて、プログラムによる方法によってのみ行われる。 • データベースへの直接アクセスまたはクエリはデータベース管理者のみに制限される。 • データベース・アプリケーション用のアプリケーションIDを使用できるのはそのアプリケーションのみである（個々のユーザーやその他の非アプリケーション・プロセスは使用できない）。	Oracle MiniClusterは、企業向けの単一テナントまたは、クラウドにあるマルチテナント・システム内の専用コンピューティング環境として設計されています。 最初のインストール時に、カード会員データを保管しているすべてのデータベースへのすべてのユーザー・アクセスに、細かな設定の可能なアクセス制御が実施されます。ユーザーには、この要件のすべての制御に適合するように権限を付与することができます。	対応または適合	CC5.1、CC5.4

PCI要件	Oracle MiniClusterの詳細	適合または対応	サポートされるSOC2の基準
10.1 システム・コンポーネントへのすべてのアクセスを各ユーザーにリンクする監査証跡を確立する。	Oracle MiniClusterの「監査ロール」に、すべての監査証跡の管理、審査、報告する権利および権限を定義できます。ロールはロール識別子ではなくユーザーIDに基づいて監査されるため、ユーザーが確実に識別され、管理者による重要データの誤用を防止できます。 Oracle Databaseでは細かな設定の可能な、条件付き監査ができるため、監査ログに含まれる不要な「ノイズ」の量を最小限に抑えながら、重要なユーザーと処理を確実に監査することができます。	対応または適合	CC5.1、CC6.1
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			
10.2.2 ルート権限または管理者権限を持つ個人によって行われたすべてのアクション			
10.2.3 すべての監査証跡へのアクセス			
10.2.4 無効な論理アクセス試行			
10.2.5 識別と認証メカニズムの使用および変更（新しいアカウントの作成、特権の昇格を含むがこれらに限定されない）、およびアカウントの変更、追加、削除のすべてはルートまたは管理者権限が必要である。			
10.2.6 監査ログの初期化、停止、一時停止			
10.2.7 システムレベル・オブジェクトの作成および削除			
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 ユーザー識別子			
10.3.2 イベントの種類			
10.3.3 日付と時刻			
10.3.4 成功または失敗を示す情報			
10.3.5 イベントの発生元			
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。			

PCI要件	Oracle MiniClusterの詳細	適合または対応	サポートされるSOC2の基準
10.4 時刻同期技術を使用してすべての重要なシステム・クロックおよび時間を同期し、時間を取得、配布、保存するために以下の要件が実施されていることを確認する。	Oracle MiniClusterでは、Network Time Protocol（NTP）サービスを利用してプラットフォーム全体の時刻を同期させます。NTPサービスをOracle MiniClusterの監視/監査機能と組み合わせることで、この要件に準拠するように構成できます。	対応	なし
10.4.1 重要なシステムが正確で一貫性のある時刻を持っている。			
10.4.2 時刻データが保護されている。			
10.4.3 時刻設定は、業界で認知されている時刻ソースから受信されている。			
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。	Oracle MiniClusterのストレージへのアクセスは、ユーザーとロールに基づくアクセス制御をはじめとするさまざまな認証手法とアクセス制御技術で制御されています。また、データベースとファイル・システムのストレージを暗号化することで、保管中のデータへの不正なアクセスをさらに厳しく防止できます。さらに、必要な場合は、Oracle SolarisとOracle Databaseの監査データを外部のストレージや処理機能にオフロードできます。	対応または適合	なし
10.5.1 仕事関連のニーズを持つ個人に監査証跡の表示を制限する。	この管理項目に適合させるために、Oracle MiniClusterはRBACと最小権限モデルを使用してあらかじめ構成されており、必要最小限の権限が付与されたロールを持つユーザーのみにログへのアクセスを許可するロールベースのアクセス制御が適用されています。なお、これはOracle SolarisとOracle Databaseの両方の監査証跡に該当します。	適合	CC5.1、CC5.4
10.7 監査証跡の履歴を少なくとも1年間保持し、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）。	Oracle MiniClusterの一元化された監視機能とログ管理機能は、この管理項目の遵守に必要な保存期間要件が満たされるようにインストール時に事前構成されます。	適合	なし

COALFIRE

結論

Oracle MiniClusterには、さまざまなハードウェアやソフトウェアを追加しなくても多数のPCI DSS要件に準拠できるように組織を支援する機能が多数組み込まれています。企業もクラウド・サービス・プロバイダも、Oracle MiniClusterの最小構成でPCI DSSのほとんどの管理項目に適合させることができます。これらの管理項目は、業界およびPCI DSSのベンチマークと構成を比較するOracle MiniClusterのコンプライアンス・ユーティリティで検証できます。

参考資料

1. Nagappan R.（2016）。Oracle MiniCluster Platform Security Deep Dive
2. Oracle（2016） Oracle MiniCluster S7-2
3. Nagappan R.（2016）。Oracle MiniCluster S7-2 Platform Security
4. Oracle（2016） Oracle MiniCluster S7-2 Frequently Asked Questions
5. Cloud Special Interest Group PCI Security Standards Council（2013）。Information Supplement:PCI DSS Cloud Computing Guidelines
6. PCI Security Standards Council, LLC（2016）、Payment Card Industry（PCI）Data Security Standard、v3.2
7. American Institute of Certified Public Accountants, Inc.（2016）、TSP Section 100
8. Oracle MiniCluster S7-2 プラットフォームのセキュリティ – テクニカル・ホワイト・ペーパー：http://www.oracle.com/jp/products/servers-storage/miniclusters7-security-3459326-ja.pdf?ssSourceSiteId=otnjp

謝辞

本書の作成に協力してくださったオラクルのRamesh Nagappanに感謝いたします。また、CoalfireのDan StockerとKevin Tamにも同じく感謝いたします。

COALFIRE

付録A- SOC2 TRUSTサービス規準

次の表は、セキュリティのためのTrustサービス原則（TSP）のTrustサービス規準をまとめたものです。

CC1.0 組織および管理に関する規準
規準
CC1.1 事業体は、対象となるTSPに関連するコミットメントを果たし要件を満たすために、システムの設計、開発、導入、運用、保守、およびモニタリングするための組織構造、指揮命令系統、権限、および実行責任を明確にしている。
CC1.2 事業体のシステム制御機能およびその他のリスク軽減策の設計、開発、導入、運用、保守、モニタリング、および承認にかかわる実行責任と説明責任を事業体内の個人に権限とともに割り当ててポリシーを守り、その他のシステム要件を効果的に施行および導入して、対象となるTSPに関連する事業体のコミットメントを果たし要件を満たしている。
CC1.3 事業体は、対象となるTSPに影響を与えるシステムの設計、開発、導入、運用、保守、およびモニタリングの担当者の適性を評価する手順を整備し、担当者が実行責任を果たす上で必要なリソースを提供している。
CC1.4 事業体は、対象となるTSPに関連するコミットメントを果たしシステム要件を満たすために、従業員の行動規範を策定し、従業員選考手続き（バックグラウンドチェックを含む）を導入し、実施手順を実行している。

CC2.0 伝達に関する規準
規準
CC2.1 システムの設計と運用、およびその範囲に関する情報を整備し、権限を有する内部および外部のシステム・ユーザーに伝達し、システムにおけるそれぞれの役割やシステム運用の結果をユーザーが理解できるようにしている。
CC2.2 対象となるTSPに関連する事業体のコミットメントを必要に応じて外部のユーザーに伝達し、この責務および関連するシステム要件を内部のユーザーに伝達し、ユーザーがその実行責任を全うできるようにしている。
CC2.3 内部および外部のユーザーおよび、システム運用に影響を及ぼす役割を持つその他の人々の実行責任をその関係者に伝えている。
CC2.4 対象となるTSPに関連するシステムの設計、開発、導入、運用、保守、およびモニタリングの内部統制に必要な情報を担当者に提供し、実行責任を遂行できるようにしている。
CC2.5 対象となるTSPに関連する障害、インシデント、懸念事項、およびその他の苦情を適切な担当者に報告する方法についての情報を、内部および外部のユーザーに提供している。
CC2.6 内部および外部のユーザーの実行責任または、対象となるTSPに関連する事業体のコミットメントおよびシステム要件に影響を及ぼすシステム変更を、適時にそれらのユーザーに伝達している。

CC3.0 リスク管理および内部統制の設計と導入に関する規準
規準
CC3.1 事業体は、（1）システムの対象となるTSPに関連するコミットメントおよびシステム要件を損なう恐れのある潜在的脅威を識別し（ベンダーおよび他のサード・パーティが提供する商品およびサービスの使用から生じる脅威、システムへのアクセス権を持つ顧客の担当者などから生じる脅威を含む）、（2）識別された脅威と関連するリスクの重大性を分析し、（3）それらのリスクに対する軽減策を決定し（内部統制の導入、商品またはサービスを提供しているベンダーおよび他のサード・パーティとその活動の評価と監視、他の軽減策を含む）、（4）内部統制システムに著しく影響する可能性のある変化（環境、規制、テクノロジーの変化および、統制状況の評価結果とモニタリング結果など）を識別して評価し、（5）識別された変化に基づいてリスク評価および軽減策を再評価し、必要に応じて改訂している。
CC3.2 事業体は、リスク軽減策を実行するための内部統制（ポリシーと手続きを含む）を設計、開発、および導入し、その統制の運用とモニタリングに基づいて、設計および導入の適合度を再評価し、必要に応じて内部統制を更新している。

CC4.0 内部統制のモニタリングに関する規準
規準
CC4.1 対象となるTSPに関連する事業体のコミットメントおよびシステム要件に照らして内部統制の設計および運用の有効性を定期的に評価し、識別された不備に関連する修正およびその他の必要な措置を適時に実施している。

CC5.0 論理的および物理的アクセス管理に関する規準
規準
CC5.1 対象となるTSPに関連する事業体のコミットメントを果たしシステム要件を満たすために、次の各項に対応する論理的なアクセスセキュリティに関するソフトウェア、インフラストラクチャおよびアーキテクチャを実装している。（1）権限を有する内部および外部のユーザーの識別と認証、（2）管理者により権限を与えられたシステム・コンポーネント（ハードウェア、データ、ソフトウェア、モバイル・デバイス、出力およびオフライン要素を含む）またはその一部への、内部および外部の権限を有するユーザーのアクセス制限、および（3）不正なアクセスの防止と検出。
CC5.2 対象となるTSPに関連する事業体のコミットメントを果たしシステム要件を満たすために、事業体がアクセス権を管理している内部および外部の新規ユーザーには、登録および承認が完了してからシステム資格証明を発行し、システムへのアクセス権を付与している。事業体がアクセス権を管理しているユーザーについては、ユーザー・アクセスが承認されなくなった時点でユーザーのシステム資格証明を削除している。
CC5.3 対象となるTSPに関連する事業体のコミットメントを果たしシステム要件を満たすために、システム・コンポーネント（インフラストラクチャ、ソフトウェア、データなど）へのアクセス時に内部および外部のユーザーを識別および認証している。
CC5.4 対象となるTSPに関連する事業体のコミットメントを果たしシステム要件を満たすために、役割、実行責任、またはシステム設計および変更に基づいて、データ、ソフトウェア、機能、および他のITリソースへのアクセスを承認および修正または削除している。
CC5.5 対象となるTSPに関連する事業体のコミットメントを果たしシステム要件を満たすために、権限を有する担当者以外はシステムを収容する施設（データセンター、バックアップ・メディア・ストレージ、その他の機密性の高い場所とそのような場所にある機密性の高いシステム・コンポーネントなど）に物理的にアクセスできないようにしている。
CC5.6 事業体のコミットメントを果たしシステム要件を満たすために、対象となるTSPに関連する脅威がシステムの範囲外にあるソースから侵入するのを防ぐ論理的なアクセスセキュリティ対策を導入している。
CC5.7 対象となるTSPに関連する事業体のコミットメントを果たしシステム要件を満たすために、権限を有する内部および外部のユーザーとプロセス以外は情報を送信、移動、および削除できないようにし、送信、移動、または削除時には情報を保護している。
CC5.8 対象となるTSPに関連する事業体のコミットメントを果たしシステム要件を満たすために、不正なソフトウェアまたは悪意のあるソフトウェアの侵入を阻止または検出して対処する内部統制を導入している。

CC6.0 システム運用に関する規準
規準
CC6.1 対象となるTSPに関連する事業体のコミットメントを果たしシステム要件を満たすために、悪意のある行動、自然災害またはエラーに起因する、対象となるTSPに関連する違反やインシデントについてのシステム・コンポーネントの脆弱性を識別、監視、および評価し、既知および新規の脆弱性を補う対策を設計、導入、および運用している。
CC6.2 事業体のコミットメントを果たしシステム要件を満たすために、対象となるTSPに関連するインシデント（論理的および物理的なセキュリティ違反、障害、識別済みの脆弱性を含む）を識別し、適切な担当者に報告し、あらかじめ整備しておいたインシデント対策手順に従って対処している。

CC7.0 変更管理に関する規準
規準
CC7.1 システム開発ライフサイクル（システム・コンポーネントの認定、設計、取得、実装、設定、テスト、修正、承認、および保守を含む）を通じ、対象となるTSPに関連する事業体のコミットメントおよびシステム要件に対応している。
CC7.2 対象となるTSPに関連するコミットメントとシステム要件との整合性を保持するために、インフラストラクチャ、データ、ソフトウェア、ポリシーおよび手続きを必要に応じて更新している。
CC7.3 対象となるTSPに関連する事業体のコミットメントを果たしシステム要件を満たすために、システム運用中や監視中に内部統制の設計または運用の有効性に不備が見つかった場合は、変更管理プロセスを開始している。
CC7.4 対象となるTSPに関連する事業体のコミットメントを果たしシステム要件を満たすために、システム・コンポーネントへの変更を認可、設計、開発、構成、文書化、テスト、承認、および実装している。