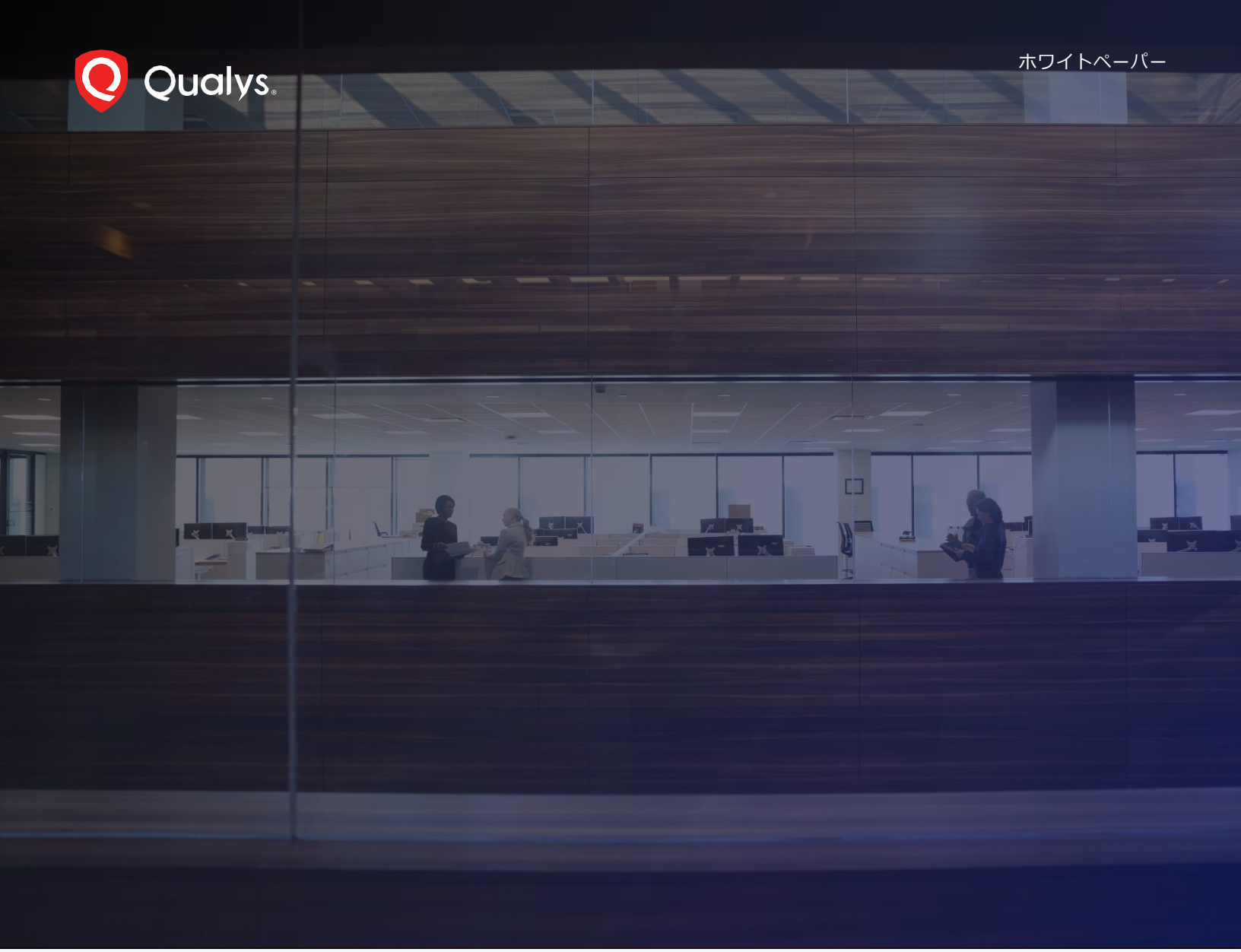
Qualys.

ホワイトペーパー



PCI DSS 4.0: 新たな要件への準拠を確保する

コンテンツ

コンプライアンスは、あらゆる規模の組織にとって継続的な要件です。義務には、国内法、国際法、政府規制、フレームワーク、特定の業界または政府機関が定める運用要件などが含まれます。

サイバーセキュリティのコンプライアンスは大きな推進力であり、その最も重要な要件の一つがPCIデータセキュリティ基準（PCI DSS）です。

業界のPCI Councilは、グローバル決済システムのセキュリティ確保を目的としてPCI DSSを策定しました。PCI DSSは、決済カード会員データ（CHD）またはセンシティブ認証データ（SAD）を保存、処理、または送信する、あるいはカード会員データ環境（CDE）のセキュリティに影響を与える可能性のあるすべての事業体に世界的に適用されます。具体的には、決済アカウント処理に関わるすべての事業体が含まれます。貴社が加盟店、プロセッサー、アクワイアラー、イシュアー、またはその他の関連サービスプロバイダーである場合、クレジットカード会社がトークン化を採用している場合でも、PCI DSSの要件を遵守する必要があります。遵守しない場合、厳しい罰則が科せられる可能性があります。ポリシーは、American Express、Discover Financial Services、JCB International、Mastercard、UnionPay、VISA, Inc.を含む執行委員会によって策定されます。

このホワイトペーパーでは、PCI DSS が決済データのセキュリティに及ぼす影響、リスクの所在、コンプライアンスに求められる要件、Qualys クラウド プラットフォームが機密データへのリスクを軽減しながらコンプライアンスの重要な要素を自動的に満たす仕組みについて説明します。

PCI DSSが今日重要な理由

PCI DSSは2004年の制定以来、決済データのセキュリティを確立・維持するための包括的かつ体系的なアプローチにより、決済業界以外でも採用されているサイバーセキュリティモデルです。様々なコンプライアンス体制を、単にチェックボックスをチェックするだけの作業だと揶揄する人もいるかもしれません。しかし、PCI DSSに準拠することで、組織は機密データに対する真のセキュリティを確保できる可能性が高まります。

言い換えれば、コンプライアンスは単なる負担ではなく、強固なセキュリティを実現するための最大の味方となり得ます。その一方で、コンプライアンスを遵守しなかった場合、クレジットカード会社は「取引停止」し、クレジットカード決済の受付を制限または停止する可能性があります。クレジットカード会社がトークン化を採用していれば、その効果はありますが、PCI DSSの要件への準拠は依然として必要となるでしょう。これは、顧客のマーケティングデータを収集している場合に特に当てはまります。PCI DSSへの準拠違反によるブランドイメージの毀損と収益リスクは非常に高く、大企業では月額最大10万ドル、小規模組織では月額5,000ドルからという罰金が科せられる可能性があります。

さらに懸念されるのは、現在、米国のほとんどの州で、カリフォルニア州消費者プライバシー法（CCPA）などの厳格な民法が制定されており、クレジットカード情報など、個人を特定できる情報（PII）を漏洩した企業には罰金や罰則が科せられることです。また、ほとんどの州では「民事訴訟」が認められており、弁護士は民間人を代表して、このような漏洩について訴訟を起こすことができます。法的証拠開示や訴訟費用は簡単に数百万ドルに膨れ上がり、ブランドイメージにダメージを与えるような報道が後を絶ちません。

専門家は、PCI DSSがサイバーセキュリティのゴールドスタンダードであると述べています。最新バージョン4.0の適用範囲は広大です。6つの戦術目標、12の主要要件、そして数百のサブ要件とテスト手順が定められており、総計356ページに及んでいます。バージョン4.0では、コンプライアンスへの2つのアプローチも導入されています。1つは、従来の「定義済み」アプローチで、技術要件とプロセス要件、そしてテスト手順を厳密に遵守します。もう1つは、リスクベースのアプローチで、カスタマイズされたプロセス、または定義されたプロセスとカスタムプロセスの組み合わせを可能にします。

セキュリティおよびコンプライアンス担当者にとって、PCI DSSコンプライアンスの追求において最も困難な点は、必要なツールとサービスをすべて提供できるベンダーが存在しないことです。そのため、PCI DSSコンプライアンスプロセスの確立と維持は、中小企業から大企業まで、複雑になる可能性があります。その理由を理解するために、潜在的な脆弱性がどこに存在し、PCI DSS 4.0が新しい要件を通じてどのようにそれらに対処しているかを考えてみましょう。

PCI DSS脆弱性リスクが存在する場所

PCI DSS 要件は、支払い処理エコシステムのあらゆる場所で発生する可能性のある脆弱性を対象としています。会社でこのような物理または仮想デバイス、システム、またはサービスを使用している場合は、注意が必要です。

- クラウドベースのシステム
- エンドポイントデバイス（モバイル、ノートブック、PC）
- 紙ベースの保管システム
- POS端末
- リモートアクセス接続
- WindowsおよびLinuxサーバー
- カード会員データをサービスプロバイダーへの送信
- サービスプロバイダーおよびアクワイアラーが運営するシステムの脆弱性
- Webショッピングアプリケーション
- ホットスポット

脆弱性は、ハードウェア、ソフトウェア、ネットワーク、アプリケーション、サプライチェーン、パートナー、サービスプロバイダーなど、他のリソースにも発生する可能性があります。決済セキュリティの実現が大きな課題となるのも当然です。PCI DSSの適用範囲がこれほど広範囲なのは、まさにこのためです。PCI DSSは、多くの分野にまたがる多数の潜在的な脆弱性に対処する必要があるからです。

PCI DSS 4.0がコンプライアンスに求める要件

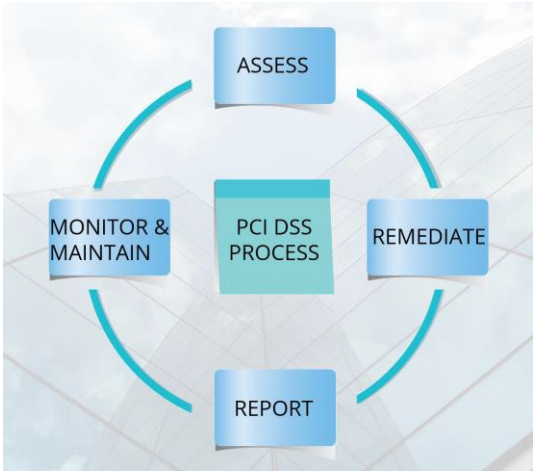
PCI DSSバージョン4.0は2022年3月に発表され、組織が遵守すべき64の要件が盛り込まれています。これらの要件は2つのフェーズに分かれており、13の要件は2024年3月31日に、残りの51の要件は2025年3月31日にそれぞれ必須となります。PCI Councilはバージョン4.0において、以下の4つの戦略目標を設定しました:

1. 決済業界のセキュリティニーズへの対応を継続します。これには、多要素認証、パスワード、eコマース / フィッシング対策に対する厳格な要件が含まれます。
2. セキュリティを継続的なプロセスとして推進します。これにより、セキュリティの実装と維持に関するガイダンスが明確になります（下記参照）。
3. 様々な手法への柔軟性を高めます。万能なソリューションは存在せず、組織によってはコンプライアンスへのアプローチに柔軟性が求められることを認識します。
4. 検証方法を強化します。コンプライアンス報告書または自己評価質問票（SAQ）とコンプライアンス証明書の整合性を強化します。

コンプライアンス達成のための４段階プロセス

PCI DSS 4.0では、PCI Councilは、組織が決済アカウントデータを保護するために実行すべき4つの継続的な手順を示しています。PCI DSSクイックリファレンスガイド「*PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 4.0* (p. 4)」, に記載されているように、これらの手順は次の通りです:

1. 評価 – 決済アカウントデータのすべての保管場所を特定し、決済処理に関連するすべてのIT資産と業務プロセスのインベントリを作成し、決済アカウントデータを漏洩させる可能性のある脆弱性がないか分析し、必要な管理策を実装または更新し、正式なPCI DSS評価を受ける。
2. 是正 – セキュリティ管理策のギャップを特定して対処し、特定された脆弱性を修正し、不要な決済データストレージを安全に削除し、安全な業務プロセスを実装する。
3. 報告 – 評価と是正の詳細を文書化し、コンプライアンス承認機関（通常はアクワイアリング銀行または決済ブランド）にコンプライアンスレポートを提出する。
4. 監視と維持 – 決済アカウントデータと環境を保護するために導入されたセキュリティ管理策が、年間を通じて効果的かつ適切に機能していることを確認する。これらの「通常業務」プロセスは、継続的な保護を確保するために、組織の全体的なセキュリティ戦略の一環として実装する必要があります。



Qualys 脆弱性管理、検出、対応（VMDR）およびQualys クラウドプラットフォームの他のアプリケーションを使用するプロセス手法は、PCIカウンシルの 4 段階プロセスと完全に整合しています。
具体的な相乗効果については、以下で説明します。

PCI DSS 4.0の目標と要件

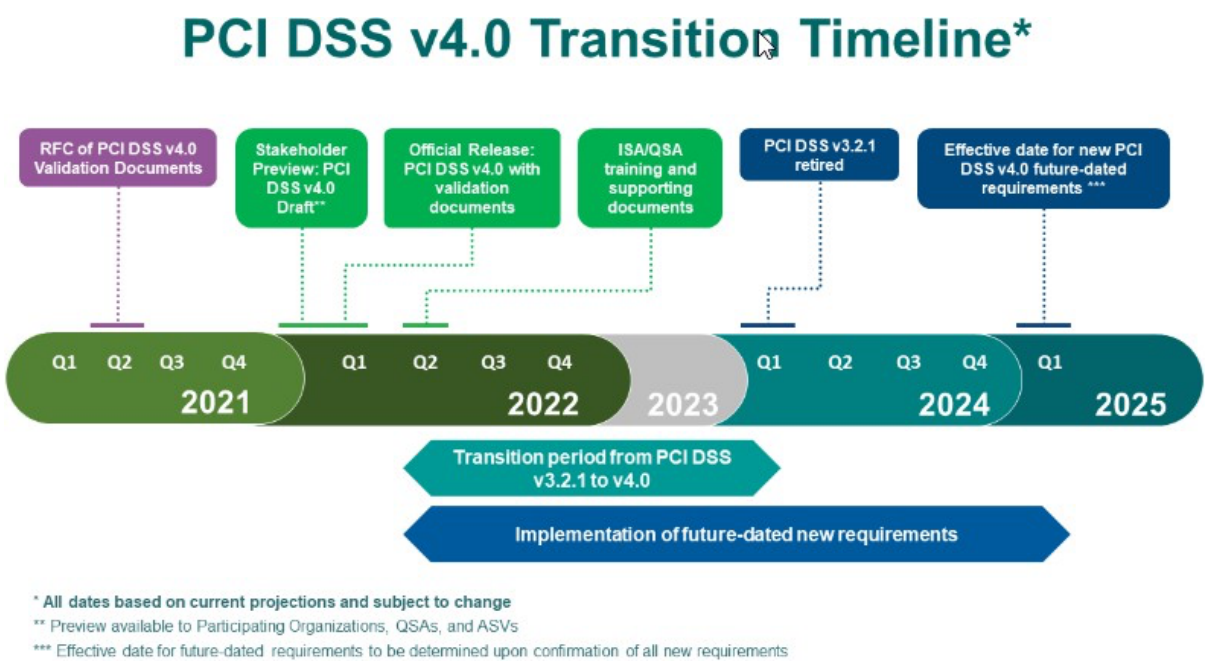
PCI DSS 4.0の大部分は、6つの戦術的目標と12の要件の明示です。以下のバージョン4.0の表では、いくつかの項目が調整されていますが、実質的にはすべて以前のバージョン3.2.1と同じです。セキュリティおよびコンプライアンスの専門家は、この表がすべての関連するコンプライアンス活動の基盤となるため、よくご存知でしょう。3つ目の目標は脆弱性管理に関するものですが、すべての目標と要件はあらゆるセキュリティプログラムの基礎であり、「サイバーセキュリティのための12ステッププログラム」に似ています。PCI Councilもこの類似点を指摘しています（クイックリファレンスガイドの8ページを参照）。そのため、組織がPCI DSS 4.0コンプライアンスのために行うすべてのことは、脅威からの保護とITエコシステム全体のセキュリティ要素の保護にも役立ちます。これは、Qualysクラウドプラットフォームがコンプライアンスだけでなく、一般的なサイバーセキュリティにも不可欠であるもう1つの理由です。

ゴール	PCI DSS要件
安全なネットワークとシステムの構築と維持	ネットワークセキュリティ管理を導入し、維持する すべてのシステムコンポーネントに安全な構成を適用する
アカウントデータの保護	保存されたアカウントデータを保護 オープンなパブリックネットワークを介した送信時に、強力な暗号化技術を使用してカード会員データを保護します
脆弱性管理プログラムを維持	すべてのシステムとネットワークを悪意のあるソフトウェアから保護する安全なシステムとソフトウェアを開発し、維持する
強力なアクセス制御対策を実施	システムコンポーネントへのアクセスを、業務上必要な範囲でカード会員データに制限する ユーザーを識別し、システムコンポーネントへのアクセスを認証する カード会員データへの物理的アクセスを制限する
ネットワークを定期的に監視およびテスト	システムコンポーネントとカード会員データへのすべてのアクセスをログに記録し、監視する セキュリティシステムとネットワークを定期的にテストする
情報セキュリティポリシーを維持	ポリシーとプログラムで情報セキュリティをサポートする

PCI DSS 4.0に準拠するための管理策とプロセスを適用するのは、大規模な作業のように思えるかもしれませんが、この規格ではセグメンテーションを用いてコンプライアンスの範囲を縮小することで、その負担を軽減しています。セグメンテーションとは、カード会員データ環境（CDE）（コンプライアンスの対象となるすべてのもの）を、組織のITインフラストラクチャ内の他のすべてのものから分離することを意味します。例えば、セグメンテーションには物理サーバー、データストレージ、ネットワークデバイスが含まれる場合があり、組織のクラウド内にあるそれらの仮想インスタンスも含まれる可能性があります。サードパーティのサービスプロバイダーの利用には、特別なセグメンテーションルールが存在します（要件12.8および付録A1を参照）。セグメンテーションを用いることで、保護対象の範囲を大幅に縮小し、残りの対象資産に対するPCI DSS検証監査プロセスを簡素化できます。

「PCIコンプライアンス」とは、PCI DSS 4.0の要件を満たすことを指します。しかし、PCI DSSは決済セキュリティに関する唯一の規格ではありません。

PCI Councilは現在、15種類のPCIセキュリティ規格を管理しています。



Data courtesy of PCI Security Standards Council

QualysがPCI DSS 4.0準拠を推進する方法

Qualys Enterprise TruRisk プラットフォームには 20 を超えるアプリケーションが含まれており、その多くは、組織が PCI DSS 4.0 への準拠を次の 2 つの方法で確保するのに役立ちます。1 つ目は、コンプライアンスの自動ドキュメント化を可能にすることです。これは、PCI DSS 4.0 要件に対する多くのコントロールが実施されているかどうか、そしてそれらがそれぞれの役割を果たしているかどうかのステータスチェックです。2 つ目は、脆弱性管理、検出と対応、Web アプリケーションスキャン、ポリシーコンプライアンス、ファイル整合性監視など、Qualys のさまざまなセキュリティアプリケーションが統合されているため、このプラットフォームは PCI DSS 4.0 要件の堅牢なサブセットに対して具体的なコントロールを提供します。

PCI DSS 4.0 などのコンプライアンスルールでは、セキュリティ関係者に 2 種類のチェック、つまり必要なコントロールが実施されていることを確認することと、コントロールが必要に応じて機能していることを確認することが求められ

ます。Qualys は、Qualys クラウドプラットフォーム用の 2 つのアプリケーションによって、このプロセスの自動化を支援します。

一部の中規模企業とほとんどの大規模企業は、PCI DSS監査を実施し、コンプライアンスを検証し、結果を正式なコンプライアンス報告書に提出するために、認定セキュリティ評価機関（QSA）を利用する必要があります。対象となるカード会員データ環境の規模と複雑さによっては、このプロセスの実行は煩雑で時間のかかる作業となる可能性があります。また、このアプローチを採用する組織は、カード会員データと機密認証データを危険にさらす可能性があります。なぜなら、必須の年次評価は、まさにその時点の測定であり、1つ以上のコントロールが不合格になった場合、数時間以内にコンプライアンス違反になる可能性があるからです。PCI Councilは関係者に対し、「コンプライアンスは必ずしもセキュリティと同じではない」と助言しています。これは、インターネットに接続されたあらゆる環境に対する24時間365日の攻撃の集中砲火によって強調されています。そのため、上記のようにコンプライアンスのための4段階の継続的なプロセスが提供されています。

以下では、Qualysのソリューションをいくつか概説し、それぞれがPCI DSS 4.0のさまざまな要件へのコンプライアンス確保にどのように役立つかを説明します。

Qualys Policy Compliance (PC) は、カード会員データ環境の継続的な評価を可能にします。Qualys PC は、PCI DSS 4.0 に対応した、すぐに使用できる要件ベースのテンプレートを提供します。このテンプレートは、対象範囲の PCI 資産の評価を自動化するセキュリティチェックで構成されています。これらのチェックは、技術的なセキュリティ設定評価要件を自動的にスキャンします。

Qualys PC は、対象範囲のさまざまなオペレーティングシステム、データベース、Web サーバー、デバイスなどをサポートします。また、認定セキュリティ評価機関との連携により、コンプライアンスレポートの自動生成など、PCI DSS の年次評価を簡素化・迅速化します。カスタムダッシュボードとレポートを作成できるため、監査人が標準以外の要件を要求した場合でも、常に監査に対応できる状態を維持できます。

ほぼすべてのセクションに、ポリシーコンプライアンス機能に関する多数の要件が規定されています。例えば、「ネットワーク接続の変更とネットワークセキュリティ管理の設定変更はすべて、要件 6.5.1 に従って承認およびテストされている」ことを保証するなどです。 Qualys PCを使用すると、セキュリティ設定の評価を自動化し、PCI DSS v4.0の技術的セキュリティ要件への準拠状況を迅速に把握できます。Qualys PCは、お客様がPCI DSS v4.0規格への準備状況を迅速に文書化するためにすぐに使用できるレポートも提供します。Qualysは、PCI DSS v4.0の要件に基づいた、すぐに使用できるテンプレートをリリースしました。このテンプレートは、PCI対象資産の評価を自動化するセキュリティチェックで構成されています。このテンプレートにより、加盟店は、さまざまな技術にわたって検証が必要な主要な技術的管理策について、PCIコンプライアンスを検証するプロセスを簡素化できます。Qualys PCは、これらのすべてのPCI管理策を自動的にスキャンし、継続的なコンプライアンスを検証するための詳細なレポートを提供できるようになりました。

Qualys Security Assessment Questionnaire（SAQ）は、PCI DSS 4.0 で規定されている自己評価質問票（SAQ）と呼ばれるツールを中規模および小規模企業が使用するのに役立ちます。リンク先で説明されているように、9 種類の SAQ があり、組織の種類と環境に対応しています。対象となる組織は、SAQ を使用して PCI DSS への準拠を自己評価できます。検証結果は、コンプライアンス証明書とともに、組織のアクワイアリング銀行または決済ブランドに提出されます。

組織は、管理者に別のエージェントを追加することなく、Qualys Compliance に含まれるアプリを使用して、必要な情報の収集と検証、および SAQ の完了のプロセスを自動化できます。ビジネスプロセス制御の自動化には、組織内外のすべての関係者が含まれます。簡略化された質問票は、ブラウザに結果を入力する適切な回答者に自動的に送信されます。事前にフォーマットされた SAQ テンプレートは、必要に応じてカスタマイズできます。回答者は、特に情報収集に人間の操作が必要な場合は、より適切に回答できる同僚に質問を電子的に委任することができます。最終的なSAQは自動的に準備され、アクワイアラーまたは決済ブランドに提出できます。Qualys SAQは、プロセスを容易かつ正確、包括

的、一元管理、拡張可能、そして組織全体で統一されたものにします。

Qualys Vulnerability Management, Detection, and Response (VMDR) – VMDR は、CDE サイバーリスク（要件 2、5、6、11）を管理するための基盤ソリューションです。CDE 脆弱性管理プログラムの 3 番目の目標、および要件 11 で求められている CDE システムとネットワークのセキュリティを定期的にテストするという要件に対応します。VMDR は、内部および外部のリスクを検出し、脆弱性に効率的に対応する能力に優れています。認証スキャンは、PCI DSS 4.0 の新しい要件です。他のスキャナーとは異なり、VMDR は証明書インベントリなどの認証スキャンを実行します。VMDR には、ASV を必要とする外部スキャンへのコンプライアンスを確保するための PCI ASV Complianceも含まれています。Qualys は認定スキャンベンダー（ASV）として、PCI セキュリティ標準協議会（PCI Security Standards Council）から、PCI DSS へのコンプライアンスを証明するために必要な四半期ごとのスキャンを実施する権限を付与されています。これにより、正確かつ効果的な PCI ASV コンプライアンスのテスト、レポート、および提出を確実に行うことができます。

Qualys Web Application Scanning (WAS) – WASは、CDE内部および外部向けWebアプリケーションの脆弱性と構成ミスを継続的に検出します（要件6、11）。このアプリケーションはWebアプリケーション内のマルウェアを検出し、公開された決済データやその他の個人情報（PII）についてDevOpsチームに通知します。

Qualys File Integrity Monitoring (FIM) – FIMは、CDE整合性モニタリングの取り組みとコンプライアンス（要件1、10、11、12）を提供します。これには、誤検知と検知されたヒットを正確に区別し、ホワイトリスト化を可能にする不正な変更や変更の検出が含まれます。Qualys FIMには、不正なファイルアクセスとエージェントレスネットワークデバイスのサポートに関するアラートを通知するファイルアクセスモニタリング（FAM）も含まれています。どちらも、新しいPCI DSS 4.0要件に準拠するために必須となっています。

Qualys CyberSecurity Asset Management (CSAM)とExternal Attack Surface Management (EASM) の組み合わせ – CSAM は、CDE のすべてのサイバー資産について、正確かつコンテキスト豊富なインベントリを提供し、セキュリティギャップを特定します (要件 2)。また、CDE の外部攻撃対象領域を完全に可視化し、制御します (要件 2、12)。

Qualys Patch Management – パッチ管理は、オペレーティングシステム、モバイルデバイス、サードパーティ製アプリケーション、さらにはカード会員データ環境内のリモートデバイスへのパッチ適用プロセス全体を自動化します (要件 1、6、10、11)。

Custom Assessment & Remediation – PCI DSS 4.0 では、API を含むすべての特注ソフトウェアおよびカスタムソフトウェアの最新のインベントリを維持することが組織に義務付けられています。CAR は、カスタム構成の導入を可能にしながら、再利用可能なカスタム検出と修復機能を作成します。

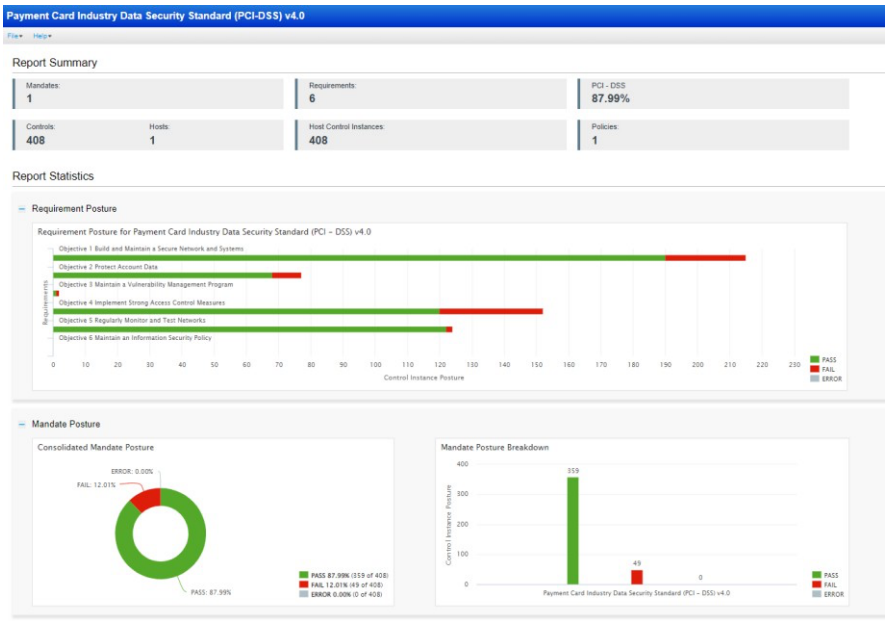
Qualys TotalCloud – PCI DSS 4.0には、アクセス制御、監視とログ記録、インシデント対応、パッチ適用とアップデート、スキャンなど、クラウド管理に関する複数の要件が含まれています。Qualys TotalCloudは、360度スキャンによるリスク測定により、脆弱性を検出し、最大99%の精度でマルウェアを検出できます。

Qualys Multi-Vector Endpoint Detection and Response (EDR) – CDEの脆弱性管理とエンドポイント脅威検出および対応を統合するには、EDRの使用が推奨されます（要件5、12）。

Qualys Context XDR – Extended Detection and Responseは、MITRE ATT&CKに基づく脅威ハンティングと分析を用いて、CDEに対する複雑で高度な脅威の修復を迅速化するために追加する必要があります（要件10）。

PCI DSS v4.0の要件テンプレートは、以下を提供します。

- 組織にとって効果的な管理と、PCI DSS v4.0の暗黙的な要件に関する迅速なレポート作成機能
- すべての技術的セキュリティ構成評価要件を網羅
- 対象範囲に含まれるさまざまなオペレーティングシステム、データベース、Webサーバー、ネットワークデバイスなどをサポート



PCI DSS 4.0 ソリューションマトリックス

以下は、PCI DSS 4.0 の要件の多くをさまざまな Qualys ソリューションにマッピングしたマトリックスと、各ソリューションが各要件への準拠をどのように保証できるかについての説明です。

PCI DSS 4.0 Requirement	Qualys App	Capabilities
1.2: Network security controls (NSCs) are configured and maintained.	Qualys PC, FIM, TotalCloud (TC)	FIMはエージェントレスネットワークデバイスをサポートします。TCはマルチクラウド環境全体におけるワークロードと設定ミスの可視化を提供します。
2.2: System components are configured and managed securely.	Qualys VMDR, PC, CSAM	VMDRは脆弱性を発見し、PCは設定ミスを検出します。CSAMは外部/内部資産の分類を行います。
2.3: Wireless environments are configured and managed securely.	Quays PC	PCはすべての環境における設定ミスを発見します。
3.3: Sensitive authentication data is not stored after authorization.	Qualys PC	PCは、機密性の高い認証データの可視性を提供することで、この要件を満たすのに役立ちます。
3.4: Access to displays of full PAN, ability to copy account data is restricted.	Qualys PC	PCはこのデータへの可視性を提供することで、この要件を満たすのに役立ちます。

3.6: Cryptographic keys used to protect stored account data are secured.	Qualys PC	PCはこのデータへの可視性を提供することで、この要件を満たすのに役立ちます。
4.2: PAN is protected with strong cryptography during transmission.	Qualys PC	PCはこのデータへの可視性を提供することで、この要件を満たすのに役立ちます。
5.2: New: Malicious malware is prevented, or detected and addressed.	Qualys PC, EDR	EDRは悪意のあるマルウェアを検知し防御します。PCはEDRで検出された設定ミスを自動修復します。
5.3: New: Anti-malware mechanisms and processes are active, maintained…	Qualys PC, EDR, VMDR	VMDRは定期的なスキャンを実行し、EDRとPCはシステムやプロセスの継続的な行動分析を提供する
6.2: Bespoke and custom software is developed securely.	Qualys VMDR, PC	VMDRとPCは、このデータに対する可視性を提供することで、この要件を満たすのに役立ちます。
6.4: Public-facing web applications are protected against attacks.	Qualys WAS	WASは、一般公開されているWebアプリケーションの保護を支援します。
6.3: Security vulnerabilities are identified and promptly addressed.	Quays CSAM, PM, VMDR, TC, PC	PMはパッチの適用を保証する。TCはクラウド脆弱性を修正し、VMDRは脆弱性を特定し、CSAMは資産を棚卸する。
6.3.1: Risk based assessment approach for vulnerability management.	Qualys VMDR	ビジネスコンテキストを組み込んだリスクベースのVMプログラムへVMを高度化 特注およびカスタムソフトウェアの脆弱性をカバー
6.5: Changes to all system components are managed securely.	Qualys PC	PCはコンポーネントの設定変更の誤りを検出するのに役立ちます。
7.2: Access to displays of full PAN, ability to copy account data is restricted.	Qualys PC, FIM	PCはこの要件を満たすのに役立ちます。FIMはロールベースのアクセス制御をサポートします。
8.2/3/4/5/6: User identification and related accounts for users…	Qualys PC	PCはこのデータへの可視性を提供することで、この要件を満たすのに役立ちます。
10.2/3/5: Audit logs are implemented to	Qualys PC, FIM	PCはこの要件を満たすのに役立ちます。FIMは、ファイルアクセス管理（FAM）およびファイル整合性に関する監査ログを維持し、カード保有者データへのユーザーアクセスを記録します。

support the detection of anomalies…		
10.4: New requirement for automated mechanisms for audit log reviews.	Qualys FIM	ファイルアクセス監視（FAM）は、完全性が変更されなくても全てのユーザーアクセスをカバーします。FIMは洞察を得るためのSIEM統合を備えています。
10.7: Failures of critical security control systems are detected, reported…	Qualys TC, FIM, PC, EDR, CAR	いくつかのアプリがこの機能をカバーします：TotalCloud、EDR、PC。FIMは、FIMソリューションの障害発生時に自動アラートとレポートを提供します。
11.3: External and internal vulnerabilities are regularly identified, prioritized…	Qualys VMDR, PC, PCI ASV	Qualys VMDR PCI ASV（VMDRに付属）は外部スキャンをカバーします。
11.3.1.2: New requirement: authenticated internal vulnerability scans.	Qualys VMDR	VMDRは内部スキャン認証の要件をカバーします。
11.4: External and internal penetration testing, exploitable vulnerabilities and security weaknesses are corrected.	Quays VMDR, PC, TC	PMはパッチの適用を保証する。PCは設定ミスを発見し、VMDRは脆弱性を特定し、CSAMは資産を棚卸する。
11.5: Network intrusions and unexpected file changes are detected…	Quays FIM, EDR, PC	PMはパッチの適用を保証します。PCは設定ミスを発見し、VMDRは脆弱性を特定し、CSAMは資産を棚卸します。PCI対象資産におけるFIMは包括的なカバレッジを提供します。
6.3.1: Risk based assessment approach for vulnerability management.	Qualys VMDR	ビジネスコンテキストを組み込んだリスクベースのVMプログラムへVMを高度化 特注およびカスタムソフトウェアの脆弱性をカバー
6.5: Changes to all system components are managed securely.	Qualys PC	PCはシステムコンポーネントの可視性を提供することで、この要件を満たすのに役立ちます。
12.1/3/4/5/8: A comprehensive information security policy…for protection of the entity's information assets…	Qualys CSAM, FIM, CAR	CSAMは、PCI DSSの対象範囲となるシステムコンポーネントのインベントリを提供します。FIMは、ファイル変更に関連する日次ログをレビュー用に提供し、手動および自動でのインシデント作成を可能にするインシデント管理ワークフローを提供します。

結論

PCI DSS 4.0へのコンプライアンスは、世界中の何百万もの組織に関係する重要なトピックです。

PCI Councilが推奨する4段階の継続的なプロセス（評価、修復、報告、監視と維持）の要件に従うことで、組織は完全なコンプライアンスへの確実な道筋を歩み、ブランドイメージの毀損、罰金、訴訟のリスクを軽減できます。さらに、組織のIT環境全体にわたる強力なサイバーセキュリティ体制も確保できるという大きなメリットもあります。このプロセスを実現する手段としてQualys Compliance Solution Setを使用すると、コンプライアンスプロセスを簡素化・自動化し、カード会員データ環境を安全に保つための統合アプリケーションが提供されます。PCI DSSの詳細については、PCIカウンシルのウェブサイトにあるPCI DSS v4.0 Resource Hubで、PCI DSS 4.0の全文とその他の関連資料をご覧ください。Qualysを使用してPCI DSS 4.0コンプライアンスを達成する方法について詳しくは、無料トライアルをご利用ください。

寄稿者:

ビル リード、Qualysプロダクトマーケティング