protiviti®
Global Business Consulting

PCI SSC、データセキュリティ基準の更新を発表

DSS 4.0は急速に進化する脅威環境に対応し、組織がコンプライアンスを達成するための方法に柔軟性を提供します。

2022年3月31日、PCI Security Standards Council（PCI SSC）は、PCIデータセキュリティ基準（DSS）の新バージョンを発表しました。PCI DSS 4.0は、ほぼ4年ぶりの改訂であり、決済業界が現在直面している脅威環境の進化に対応したメジャーアップデートとなります。

今回の改訂の背景には、クラウドやその他の新技術の採用が急速に拡大し、現在の環境に合わせた基準全体の更新が必要となったこと、また、新たな脅威に対応するための要求事項の強化や、準拠検証に関して追加的な手引きを提供する必要性が増していたことがあります。

規格の変更点

PCI DSS 4.0の更新は、新たな脅威や技術への適応を行い、引き続き決済業界のセキュリティニーズに応えることを可能にします。また、技術革新をサポートするよう、組織がコンプライアンス要件を満たすための独自のアプローチを採用することを可能にするような柔軟性が追加されています。

その他、バージョン4.0の改訂点は以下の通りです。

- 冗長なテスト手順の削除、要求事項の番号変更、同じ意図を持つ要求事項の統合、異なる意図を持つ要求事項の分離など、規格自体の構造的な変更
- 導入部（「概論」）と個別要求事項へのガイダンスの追加
- 曖昧な要件とテスト手順の明確化

「カスタマイズアプローチ」と「定義されたアプローチ」

PCI DSS 4.0における最も大きな変更点の1つは、カスタマイズアプローチ（Customised Approach）と呼ばれる代替的な検証手法が新たに設けられたことです。このアプローチでは、PCI DSSが要件の目的のみを定義し、企業にとって最適な方法で目的を達成するような柔軟性が与えられます。企業はコントロールを設計し、リスク評価を実施し、コントロールを実装し、その有効性をテストしなければなりません。カスタマイズアプローチを使用する場合、PCI DSS 4.0に概説される要件に従ってすべての手順を文書化し、準拠の検証の際に認定セキュリティ評価者（QSA）によるレビューを受ける必要があるため、これまでのテストのサポートよりも正式な文書化が必要になります。QSAは、カスタマイズアプローチにより設計されたコントロールが目的を満たしていることを確認することに加え、独自に適切なテスト手順を導き出し、コントロールが適切に機能していることを確認するためのテストを行う必要があります。

これに対して、定義されたアプローチは、管理・試験手順が定義されている、これまでの検証プロセスに従ったものです。これは、PCI DSSのさまざまなバージョンに長年存在してきた、おなじみのテスト方法と同じものです。定義済みアプローチは、定義された統制が実施されて、より体系的なガイダンスを希望する組織に最適な方法です。カスタマイズアプローチと対照的に、定義済みアプローチでは、旧バージョンのPCI DSSで使用されていたのと同様に、代替コントロールの使用が許可されています。

組織は、同じテストにおいて、要件ごとに定義されたアプローチとカスタマイズアプローチを組み合わせることができ、環境の異なるコンポーネントに対して異なるアプローチを活用することもできます。

自己評価によってPCI DSS準拠を検証する事業者は、カスタマイズアプローチの対象にはなりません。

その他の注目すべき変更点および要求事項

PCI DSS 4.0はより正確を期しており、期限に関する要件のあるコントロールについて時間枠をより明確に定義しています。定期的な実施が求められるコントロールでは、事業者側がその実施を決定する期間を正当化するために、正式な定義および文書化されたリスク分析の裏付けを必要とします。また、各PCI DSSの12の要件に、それぞれの要件に含まれるすべての活動に対して役割および責任を割り当てることを義務付けています。

以下は、新たな要件を満たすために、特別な計画や、新しいソリューションやプロセスの導入が必要となる可能性があるものです。組織は、基準のすべて変更の点について、公表されたPCI DSS 4.0を参照する必要があります。

- PCI DSS 4.0では、事業者が正式にPCI準拠の適用範囲を確認することが義務付けられています。この確認は、それぞれのPCI DSS要件（要件12.5.2）で規定される詳細レベルで文書化する必要があります。

- 文書化された権限と正当かつ定義されたビジネスニーズを持つ担当者を除き、リモートで接続する担当者のカード番号情報の複製や移動を防止するために、技術的コントロールを実施する必要があります（要件3.4.2）。PCI 3.2.1では、これは技術的コントロールを求めないポリシーのみの要件でした。

- カード会員情報の暗号化に、ディスクレベルの暗号化のみを使う方法は、リムーバブルメディアにのみ許容されるようになりました。取り外し不可能なメディアに保存されたカード会員データは、PCI DSS要件（要件3.5.1.2）を満たすために他の手段で追加的に暗号化する必要があります。

- フィッシングやソーシャル・エンジニアリング攻撃は、攻撃者が侵入を成功させるために活用する主要な攻撃経路の1つです。PCI DSSソーシャル・エンジニアリングの検出、防御するための技術的コントロールの要求（要件5.4.1）、セキュリティ啓発トレーニングにフィッシングおよびソーシャル・エンジニアリングの脅威に関する教育を含めることを組織に求めています（要件12.6.3.1）。

- インターネットに接続するすべてのウェブアプリケーションを保護するために、ウェブアプリケーションファイアウォール（WAF）が必須となりました（要件6.4.2）。PCI DSSの前バージョンでは、手動または自動のアプリケーション脆弱性セキュリティ評価ツールによる公開用Webアプリケーションのレビューを活用し、WAFに代わる手段を提供していました。

アクセス制御要件の強化

以前のバージョンのPCI DSSでは、システムおよびアプリケーションのアカウントについて言及されていませんでしたが、PCI DSS 4.0では、システムおよびアプリケーションのアカウントの厳格な管理に関するいくつかの新しい要件（要件7.2.5）と、定期的なレビュー（要件7.2.5.1）およびパスワード保護（要件8.6.1）が含まれています。組織は、対話型ログインに使用できるアプリケーションおよびシステムアカウントが、スクリプト、設定／プロパティファイル、またはカスタムソースコードにハードコーディングされないようにしなければなりません（要件8.6.2）。静的コード解析ツールは、コード内にハードコーディングされたパスワードを発見するのに役立ちます。また、データ損失防止（DLP）ツールを使用して、スクリプトや設定ファイル内の認証情報を検索することもできます。

ユーザーアカウントは、ユーザーが正当であり、適切なアクセスが与えられていることを確認するために、6ヶ月ごとにレビューされる必要があり、文書化される必要があります（要件7.2.4）。Sarbanes-Oxley法（SOX法）に準拠する組織は、SOX法のために確立された既存の四半期ごとのアカウントレビュー手順を活用することができるかもしれません。同じプロセスをシステム／アプリケーションのアカウントにも適用しなければならなりませんが、これらのアカウントは、文書化されたリスク分析による定義された頻度で、「定期的に」レビューされる可能性があります。

多要素認証（MFA）の使用要件が拡張され、カード会員データ環境へのすべてのアクセスにMFAを必要とするようになりました（要件8.4.2）。また、PCI DSS 4.0で、MFAはワンタイムトークン方式のようにリプレイ攻撃の影響を受けないように、また、期間限定で特別に許可されない限り管理者を含むすべてのユーザーがバイパスできないように、実装されなければならないと明記しています（要件8.5.1）。また、新しい要件では、アクセスを許可する前に、すべての認証要素を確認することが求められています。同時に、カード会員データ環境（CDE）内にない対象システムコンポーネントへのアクセスには、MFAは必要ありません。

モニタリングの要求事項の強化

PCI DSSに準拠する組織には、セキュリティ情報イベント管理（SIEM）の実装が求められるようになりました（要件10.4.1.1）。SIEMは、セキュリティイベントを監視し、潜在的なセキュリティインシデントを特定するための有効な手段であり、業界ですでに広く浸透しています。

PCI DSS 4.0では、ファイアウォール、侵入検知システム（IDS）および侵入防止システム（IPS）、改ざん検知ソリューション、マルウェア対策ツール、論理アクセス制御、物理アク

セス制御など重要なセキュリティ制御の障害を監視する要件が、サービスプロバイダのみならずすべての事業者に適用されるよう拡大されています。SIEMやセキュリティテストツールの監視や障害対応が要件に追加されました（要件10.7.2）。また、重要なセキュリティ対策の障害に対する対応の必要構成要素を定義した追加要件が、サービスプロバイダだけでなく、すべての事業者に適用されるようになりました（要件10.7.3）。

決済ページのセキュリティの強化

決済ページのセキュリティを保護するため、PCI DSS 4.0では新たに2つの要件を導入しています。決済ページで読み込まれるスクリプトはすべて、インベントリ管理を行い、権限を付与し、決済ページの各スクリプトの整合性を確認する方法を備えていなければなりません（要件6.4.3）。この要件の範囲は、決済ページそのものであり、ウェブサイトの他の部分ではないことに留意することが重要です。この要件は、広告やチャットボットなどサードパーティーが提供するものを含め、決済ページ内で読み込まれるあらゆるスクリプトに適用されます。決済ページのスクリプトが必要な場合は、SRI（Subresource Integrity）やCSP（Content Security Policy）を活用して、要件を満たすことができます。

もう一つの新しい要件は、クライアントのブラウザが受信したHTTPヘッダーと決済ページのコンテンツが無許可で変更された場合に、組織に警告する変更検知・改ざん検知のメカニズムを実装することを求めています。この対策は、受信したHTTPヘッダーと決済ページを少なくとも毎週、または事業者が文書化されたリスク分析を実施することで行われる頻度で評価しなければならなりません（要件11.6.1）。この要件を満たすために、組織は、ウェブアプリケーションとユーザーのインタラクションのシミュレーションを行う合成モニタリングツールを活用することができます。また、CSPの違反やCSPへの変更を利用して、改ざんの疑いを検出することもできます。

レガシーシステムのアップグレード

レガシーシステムやサポート切れシステム（EOLシステム）の脆弱性によるセキュリティ上の問題は、セキュリティ専門家の間ではよく知られています。PCI DSS 4.0では、使用中のハードウェアおよびソフトウェア技術について、サポートやセキュリティ修正を行うために、各ベンダーによる技術のサポート終了やEOLの発表を確認する新たな要件が導入されました。また、レガシー技術の改善計画を文書化し、経営幹部の承認を得ることも要求されます（要件12.3.4）。コンプライアンスを徹底するために、組織はタイムリーなアップグレードのための予算と計画を立てる必要があります。延長サポートがある場合は、要件を満たすための1つの選択肢となる可能性があります。

準拠の維持

PCI DSS 4.0で導入されたもう一つの重要な要件は、3カ月ごとにレビューを実施し、担当者がすべてのセキュリティポリシーと運用手順に従って業務を遂行していることを確認することです。この要件は、レビューが所定の業務の実行責任者以外の者によって実施され、レビューの結果が有効ではないことが判明した業務に対して是正措置を取るとともに文書化することを義務付けています（要件12.4.2）。レビューの結果は、PCI DSSコンプライアンスプログラムの責任者によって署名される必要があります（要件12.4.2.1）。内部監査チームは、PCIコンプライアンスを維持する担当部門から独立しており、文書化及び裏付けとなる証跡の要求事項を理解しているため、レビューを実施する最適な立場にいると言えます。この要求事項を遵守することで、QSAによる年次評価がより予測しやすくなり、コンプライアンス違反の事項も少なくなる可能性があります。

刻々と迫る移行期限

PCI SSCは、新しいPCI DSS規格で導入された多数の重要な変更点を認識し、バージョン3.2.1からバージョン4.0への移行スケジュールを確立しました。このスケジュールでは、PCI DSS 3.2.1は、2024年3月31日までの2年間有効です。この日から、PCI準拠を検証するためのすべての新しいテストでは、PCI DSS 4.0を使用する必要があります。また、ほとんどの新しい要求事項は、2025年3月31日まではベストプラクティスとして推奨される事項とみなされますが、この日を過ぎると必須となる予定です。2024年3月31日に義務付けられる新しい要件は、各セクションのアクティビティの役割と責任を割り当て文書化すること、カスタマイズアプローチで行う「ターゲットリスク分析」を実施すること、およびPCIの準拠適用範囲を毎年文書化して確認することのみになります。

企業が備えるべきこと

PCI DSS 4.0の新要件のほとんどが準拠を義務付けられるまでまだ3年近くありますが、新要件の数や更新された基準の実装に必要なリソースを考えると、組織はできるだけ早く新要件に対するギャップ評価を実施して準備を開始する必要があります。コンプライアンスギャップが特定されたら、新しい要件が有効となる前にギャップを解決し、一定期間で統制が有効に機能していることを実証できるよう、是正計画を策定する必要があります。

改善策の計画にあたっては、適用範囲を縮小できるかの検

討のほか、PCI DSS 4.0で導入された「カスタマイズアプローチ」が自組織にもたらす潜在的なメリットも検討する必要があります。また、事業者が計画している既存のプロジェクトや取り組みは、新たに公開されたPCI DSS基準に照らして評価する必要があります。プロジェクトによって、要件に対応するためにスコープを調整する必要があれば、期限までにコンプライアンス要件を確実に達成するために優先順位を変更する必要がある場合もあります。

新たに必要となるプロセスを運用するために十分な能力があることを確かのものとできるよう、人員配置とトレーニングレベルを分析する必要があります。例えば、ユーザーアカウントの半期ごとのレビューや、システム及びアプリケーションアカウントの定期的なレビューのプロセスに追加のリソースが必要になる場合があります。PCI DSS で要求されるタスクが意図したとおりに実行されていることを確認するために 3 か月ごとに正式なレビューを実施する必要があります。これらのレビューを実施するためのリソースを特定する必要があるだけでなく、レビューを担当する要員が評価を実施するための資格やトレーニングを取得することを確認する必要があります。独立性の観点から見ると、内部監査部門がレビューを担当するのが最適ですが、内部監査チームの中にPCI の内部レビューを実施するために、スキルアップが必要となる部分もあるでしょう。

レガシーシステムやサポート切れシステムが組織内にまだ多く存在していることを考えると、時代遅れの技術を是正するための要件は、企業にとって多面的なアプローチを必要とする可能性があります。それには、リソースの強度をアップグレードするだけではなく、プロセスの変更、アウトソーシング、レガシー技術に依存するコアビジネスアプリケーションが適時にアップグレードできない場合の代替コントロールも含まれる可能性もあります。

プロティビティの支援

プロティビティは、PCI SSC（PCI Security Standards Council）が設立される前の2002年にデータセキュリティ基準が制定されて以来、PCIに携わっています。当社は、最大かつ最も経験を持つQSA企業の1社として、多くの業界の中堅以上の組織からフォーチュン500社までの顧客に対して、数多くのPCIコンプライアンス評価を完了しています。

プロティビティは、以下のプログラムにおいて、PCI SSCの認定を受けたグローバルプロバイダーです。

- 認定セキュリティ評価機関（QSA）
- 決済アプリケーション向け認定セキュリティ評価機関（PA-QSA）
- 認定PINセキュリティ評価機関（QPA）

プロティビティのグローバルなPCIプランニング、レディネス、コンプライアンスの専門家が、お客様の組織と協力してPCI 4.0準拠のギャップ評価を実施し、どの要件が現在実施されておらず是正が必要なのかを理解します。そして、新しいソリューションの導入、プロセスの変更やアウトソーシング、代替コントロールの導入、一部の要件に対するカスタマイズアプローチの計画など、コンプライアンスを徹底するための最も効果的かつ効率的な方法についてアドバイスを提供します。また、以下サービスも提供します。

- 年1回のオンサイト評価
- 四半期ごとの脆弱性スキャン
- 年1回のペネトレーションテスト
- プログラムガバナンスおよび技術的是正の支援
- Visa PIN Securityのレビュー

プロティビティについて

プロティビティは、企業のリーダーが自信をもって未来に立ち向かうために、高い専門性と客観性のある洞察力や、お客様ごとに的確なアプローチを提供し、ゆるぎない最善の連携を約束するグローバルコンサルティングファームです。25ヶ国、85を超える拠点で、プロティビティとそのメンバーファームはクライアントに、ガバナンス、リスク、内部監査、経理財務、テクノロジー、オペレーション、データ分析におけるコンサルティングサービスを提供しています。プロティビティは、Fortune 1000の60％以上、Fortune Global 500の35％の企業にサービスを提供しています。また、成長著しい中小企業や、上場を目指している企業、政府機関等も支援しています。プロティビティは、1948年に設立され現在S&P500の一社であるRobert Half International（RHI）の100%子会社です。

© 2022 Protiviti Inc. All rights reserved. 複写禁、転載禁

protiviti®