Security Standards Council™

補足情報: 要件 11.3 ペネトレーションテスト

リリース: **2008-04-15**

全般

PCI DSS 要件 11.3 では、ペネトレーションテストが取り上げられています。これは、PCI DSS 要件 11.2 で要求されている内部と外部の脆弱性監査とは異なります。脆弱性監査では、目立った脆弱性を特定して報告するのみで、ペネトレーションテストではこれらの脆弱性に攻撃を試み、不正アクセスなどの悪意のある行為が可能かどうかを判断します。ペネトレーションテストでは、ネットワークとアプリケーションに関連する管理と処理の他に、ネットワーク層とアプリケーション層のテストが必要です。また、ネットワーク外部からの侵入（外部テスト）とネットワーク内部からの漏えいの両方に対して実施する必要があります。

ペネトレーションテストの実施者

PCI DSS では、QSA や ASV によるペネトレーションテストの実施を必須としてはいません。組織内の有資格者か、資格のある第三者による実施が望ましいでしょう。組織内の人員がペネトレーションテストを実施する場合は、ペネトレーションテストの経験が豊富な人材を選ぶ必要があります。ペネトレーションテストは、テスト対象環境の管理に関与していない人が実施しなければなりません。たとえば、ファイアウォール管理者がファイアウォールのペネトレーションテストを実施すべきではありません。

報告と文書化

ペネトレーションテストの方法と結果は文書化しておくことをお勧めします。PCI SSC ではペネトレーションテストの報告を必須としてはいませんが、テスト結果を保管しておけば、確認された問題を追跡したり、別の者が PCI DSS 監査を実施する際に証拠として参照できます。

範囲

ペネトレーションテストの実施範囲は、カード会員データ環境と、この環境に接続するすべてのシステムとネットワークです。他のシステムからカード会員データ環境が隔離されるようなネットワーク区分が設定されていたり、こうしたネットワーク区分が PCI DSS 監査の一部として検証されている場合は、ペネトレーションテストの範囲をカード会員データ環境のみに限定することができます。

頻度

ペネトレーションテストは、少なくとも 1 年に 1 回は実施する必要があります。さらに、インフラストラクチャまたはアプリケーションの大きなアップグレードや変更（新しいシステム構成要素のインストールおよび設置、サブネットワークの追加、Web サーバの追加など）があった場合には実施しなければなりません。ここで言う「大きな」（アップグレードや変更）とは、特定の環境の構成によって大幅に異なるため、PCI SSC では定義できません。アップグレードまたは変更によってカード会員のデータに影響が及んだり、カード会員のデータにアクセスできるようになる場合、それは大きなアップグレードまたは変更と見なされます。他のデータや機能からカード会員データが明確に隔離されている、高度にセグメント化されたネットワークでは、どの人員や装置からもカード会員のデータにアクセスできる可能性のあるフラットなネットワークとは事の重大さが非常に異なります。セキュリティ上のベストプラクティスとして、すべてのアップグレードと変更に際してペネトレーションテストを実施し、設置されるコントロールがアップグレードや変更の後も効果的に機能することを確認する必要があります。

準備

ペネトレーションテストを実施するには、いくつかの方法があります。まずは、テスト対象システムについてどの程度の知識があるテスターを選択するかを決める必要があります。予備知識の一切ない状態でのテストは「ブラックボックステスト」として知られています。このテストでは、テスターは、最初にシステムの場所

を特定してから攻撃を試みることになります。明確な知識がある状態でのテストは、「ホワイトボックステスト」として知られています。

テスターに予備知識を与えた方がいいと判断される場合は、別の PCI DSS の必要条件であり、情報源として使用できるアイテムがいくつかあります。これらの PCI DSS のアイテムは次のとおりです。

- ネットワーク図（1.1.2）
- QSA レビューまたは自己問診（SAQ: Self-Assessment Questionnaire）の結果
- 脆弱性を特定して不正アクセスを阻止するための、毎年のコントロールテスト（11.1）
- 四半期ごとの外部と内部の脆弱性スキャンの結果（11.2）
- 前回のペネトレーションテストの結果（11.3）
- リスク評価につながる、毎年の脅威と脆弱性の特定（12.1.2）
- 毎年のセキュリティポリシーの見直し（更新が必要なポリシーによって、組織内の新しいリスクが特定される場合があります）（12.1.3）

上記のすべてにおいて、作成された文書を評価する必要があります。また、通常の監査プロセスの間に発見された脅威と脆弱性も含まれるよう考慮しなければなりません。

方法

脅威と脆弱性が評価されたらテストを計画し、環境全体から特定されたリスクに対処するためのテストを設計します。組織の複雑度とサイズに適したペネトレーションテストを計画する必要があります。カード会員のデータが保管されているすべての場所、カード会員のデータの保存、処理、転送を行うすべての主要アプリケーション、すべての主要なネットワーク接続、すべての主要なアクセスポイントを含める必要があります。ペネトレーションテストでは、ネットワークレベルと主要アプリケーションの両方への侵攻を試し、カード会員のデータ環境全体にわたる脆弱性の攻撃を試みる必要があります。ペネトレーションテストは、主要システムとファイルへの不正アクセスを実行できるかどうかを判断することを目的としています。アクセスできた場合は、脆弱性を修正する必要があります。そして、問題のないテスト結果が得られ、不正アクセスなどの悪意のある行為を実行できなくなるまでペネトレーションテストを繰り返す必要があります。

構成要素

ソーシャルエンジニアリングおよび露呈した脆弱性の攻撃や、主要システムと主要ファイル、Web に面したアプリケーション、カスタムアプリケーション、無線接続へのアクセス制御など、これらすべてのペネトレーションテスト技法が（他のものと同様に）テスト方法に盛り込まれるよう考慮してください。

重要事項

- **PCI 準拠に関して、リソース（ネットワークまたはサーバ）の可用性を標的にした DoS 攻撃を引き起こすおそれのある脆弱性または誤構成のテストは、ペネトレーションテストに含めないでください。こうした脆弱性は、カード会員のデータを脅かすことはないと考えられます。**
- ペネトレーションテストのタイミングと範囲について、影響を受ける組織内の関係者全員に連絡してください。
- 変更管理、ビジネス継続性、障害回復などの重要な企業プロセスに従ってテストを実施してください。
- すべてのペネトレーションテストは、保守ウィンドウを監視しながら実施してください。

PCI Security Standards Council について

PCI Security Standards Council の任務は、PCI データセキュリティ基準をはじめとする、支払いデータのセキュリティを高める各種基準についての教育と認知を促進することにより、支払口座のセキュリティを強化することです。

PCI Security Standards Council は、ペイメントカードの大手ブランドである American Express、Discover Financial Services、JCB International、MasterCard Worldwide、Visa Inc. によって設立されました。すべての利害関係者が、継続中の PCI Data Security Standard（DSS）、PIN Entry Device（PED）、セキュリティ要件、Payment Application Data Security Standard（PA-DSS）の開発、強化、普及に対してアドバイスし合える、透明性のある評議会を開催することを目的としています。加盟店、銀行、プロセサー、POS ベンダの皆様は、ぜひ参加組織としてご加入ください。