PCI DSS（Payment Card Industry Data Security Standard）コンプライアンス

PCI DSS のアプリケーション・セキュリティに関する要件への対応を支援

PCI DSS（Payment Card Industry Data Security Standard）は、カード会員データを保存、処理、転送する事業者に適用されるデータ・セキュリティ基準です。これらの事業者が PCI DSS へのコンプライアンスを達成するには、セキュア・アプリケーションの開発とデプロイに関する要件を満たす必要があります。これらの要件を満たして PCI DSS へのコンプライアンスを達成していただけるよう、ブラック・ダックはさまざまな製品、サービス、トレーニングを提供しています。

概要

ブラック・ダックは、アプリケーション・セキュリティ、ネットワーク・ペネトレーション・テスト、およびセキュア・コード・レビューに関する PCI DSS の要件（6.3、6.5、6.6、6.7、11.3）への対応を支援しています。ソフトウェア・セキュリティに対する戦略的アプローチをご希望の場合は、PCI DSS の要件への対応にも役立つソフトウェア・セキュリティ・イニシアティブ（SSI）作成のお手伝いをします。ブラック・ダックが提供するソリューションには、以下のものが含まれます。

- 製品（PCI DSS 6.3、6.6）
  - **Coverity 静的解析：**開発者がコーディング中に品質上の不具合や脆弱性を高い精度で検出し、修正できます。
  - **Black Duck ソフトウェア・コンポジション解析：**バイナリ、オープンソース、サードパーティ・コードに潜むライセンス・コンプライアンスの問題や既知の脆弱性を発見します。
  - **Seeker インタラクティブ・アプリケーション・セキュリティ・テスト：**データ漏洩につながる恐れのある脆弱性を特定して検証します。
- マネージド・サービス（PCI DSS 6.3、6.6）
  - **静的アプリケーション・セキュリティ・テスト（SAST）：**ソース・コードをスキャンして、ソフトウェアの脆弱性を体系的に特定し、除去します。
  - **動的アプリケーション・セキュリティ・テスト（DAST）、ペネトレーション・テスト：**動作中の Web アプリケーションに対して自動および手動のペネトレーション・テストを実行し、脆弱性を特定します。
- ソフトウェア・セキュリティ・トレーニング（PCI DSS 6.5）
  - **e ラーニング：**開発チームに、よりセキュアなソフトウェア開発に必要なスキルと手法を提供します。
- プロフェッショナル・サービス
  - **プログラム設計と開発（PCI DSS 6.3、6.5、6.7）：**ソフトウェア・セキュリティ・イニシアチブ（SSI）の定義、実装、および測定を支援します。
  - **セキュア・コーディング・ガイドライン：**（PCI DSS 6.3、6.5、6.7）リスクの軽減、およびセキュア・コーディング手法に関する具体的なガイダンスを開発者に提供します。
  - **ネットワーク・ペネトレーション・テスト：**（PCI DSS 11.3）内部および外部公開されたネットワークに潜む脆弱性を特定し、軽減のための明確な戦略を提示します。指示に従い、すべてのネットワーク・テストにセグメンテーション・バリデーション・テストが含まれます。

これらの要件は、セキュアなアプリケーションをデリバリおよびデプロイする方法について説明しています。PCI DSS へのコンプライアンスを達成するには、これらの要件を満たす必要があります。

利点

- コーディング中にセキュリティ・ガイダンスを提示し、セキュリティを組み込む方法の学習を促すことで、開発者の効率を高めます。
- 独立したコード・レビューによるソフトウェア脆弱性の特定、定期的なカスタム・アプリケーション・コード・レビューのためのプロセス作成、更新されたコードの再評価を実施します。
- グローバルに展開するブラック・ダックのアセスメント・センター（AC）および多岐にわたる DAST ソリューションにより、ペネトレーション・テストの実装、改良、拡張を支援します。
- ユーザーのセキュリティ態勢を直ちに改善し、スタンダード、ツール、トレーニングの提供を通じ、ソフトウェア・インテグリティの継続的な改善の道筋をつけます。
- 部門横断的にソフトウェア・セキュリティの意識向上、導入、効率化を推進します。

PCI DSS の主な要件	ブラック・ダックのサービス / 製品
2.4 PCI DSS の範囲内でシステムコンポーネントのインベントリを維持します。	• Black Duck ソフトウェア・コンポジション解析
6.3 内部および外部ソフトウェアアプリケーション（アプリケーションへの Web ベースの管理アクセスを含む）を次のように開発する。 • PCI DSS（安全な認証やロギングなど）に従って。 • 業界基準やベストプラクティスに基づいて。 • ソフトウェア開発ライフサイクル全体に情報セキュリティを組み込む。	• Coverity 静的解析 • Black Duck ソフトウェア・コンポジション解析 • Seeker インタラクティブ・アプリケーション・セキュリティ・テスト • マネージド・セキュリティ・テスト • アーキテクチャ・リスク解析 • プログラム設計と開発
6.5 ソフトウェア開発プロセスにおいて次のようにして一般的なコーディングの脆弱性に対応する。 • 開発者に対して一般的なコーディングの脆弱性を回避する方法を含む安全なコーディング技法について少なくとも年に一度トレーニングを実施する。 • 安全なコーディングガイドラインに基づいてアプリケーションを開発する。	• セキュア・コーディング・ガイドライン • ソフトウェア・セキュリティ・トレーニング • プログラム設計と開発
6.6 一般公開されている Web アプリケーションについて、新たな脅威や脆弱性に継続的に対処する。また、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して、既知の攻撃から保護されていることを確実にする。	• Coverity 静的解析 • Black Duck ソフトウェア・コンポジション解析 • Seeker インタラクティブ・アプリケーション・セキュリティ・テスト • マネージド・セキュリティ・テスト
6.7 安全性の高いシステムとアプリケーションを開発・保守するためのセキュリティ・ポリシーと操作手順が文書化されて使用されており、影響を受ける関係者全員に知られていることを、確実にする。	• プログラム設計と開発 • セキュア・コーディング・ガイドライン
11.3. 外部および内部ペネトレーション・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後に実行する。セグメンテーションを用いて CDE を他のネットワークから分離した場合、少なくとも年に一度とセグメンテーションの制御 / 方法が変更された後にペネトレーション・テストを行う。	• ネットワーク・ペネトレーション・テスト
12.3 重要なテクノロジーのポリシーを作成し、これらのテクノロジーの適切な使用を定義する。	• Black Duck ソフトウェア・コンポジション解析 • プログラム設計と開発
12.6 きちんとしたセキュリティ意識向上プログラムを実装して、すべての担当者にカード会員データのセキュリティ・ポリシーと手順を認識させます。	• ソフトウェア・セキュリティ・トレーニング

ブラック・ダックについて

ブラック・ダックは、業界で最も包括的かつ強力で信頼できるアプリケーション・セキュリティ・ソリューション・ポートフォリオを提供します。ブラック・ダックには、世界中の組織がソフトウェアを迅速に保護し、開発環境にセキュリティを効率的に統合し、新しいテクノロジーで安全に革新できるよう支援してきた比類なき実績があります。ソフトウェア・セキュリティのリーダー、専門家、イノベーターとして認められているブラック・ダックは、ソフトウェアの信頼を築くために必要な要素をすべて備えています。詳しくは www.blackduck.com/jp をご覧ください。

ブラック・ダック・ソフトウェア合同会社

www.blackduck.com/jp