BLACKDUCK®

ガイド

# ペネトレーション・テスト：選び方ガイド

## ペンテストはどれも同じか？

外部からの攻撃によるものか内部不正によるものかを問わず、情報漏えいは組織にとって深刻な脅威であり続けています。IBM が発表した「2020 年データ侵害のコストに関する調査」によると、情報漏えいの 52% は悪意のある攻撃によって発生しており、情報漏えい 1 件あたりの総コストは平均 386 万ドルに達しています。これら情報漏えいの多くはさまざまなエラーや脆弱性が複合的な要因となって発生しており、システムに侵入した攻撃者は見つかる限りの弱点を悪用します。

これは、重要情報の漏えいを引き起こして企業のブランド・イメージを失墜させてしまう前に、アプリケーションとネットワークを保護することが組織にとって急務であることを示唆しています。そこで、開発およびアプリケーション・セキュリティ（AppSec）チームは静的アプリケーション・セキュリティ・テスト（SAST）やソフトウェア・コンポジション解析（SCA）などさまざまな診断手法を使用して、ネットワークおよびアプリケーションを保護します。

しかし、実行時テストやリリース・フェーズでなければ検出できない脆弱性も数多く存在します。SAST や SCA などのツールを使用すると脆弱性が存在するコード行まで特定できますが、実行時あるいは環境のリスクは特定できず、システムに存在するマルチベクトル型攻撃の脆弱性の全体像を把握することはできません。このため、多くの組織が QA フェーズや開発の最終ステージ、そして場合によってはデプロイ後に動的アプリケーション・セキュリティ・テスト（DAST）やペネトレーション・テストを使用して、開発サイクル早期には見つけることのできない脆弱性を検出しています。

### ペネトレーション・テストのフェーズ

- **偵察：**公開および非公開のソースからなるべく多くの情報を収集し、ターゲットのアタック・サーフェスと潜在的な脆弱性をマッピングします。
- **スキャン：**ターゲットの web サイトやシステムにオープン・サービス、アプリケーション・セキュリティの問題、オープンソース脆弱性などの弱点がないか検査します。
- **アクセス取得：**最適なツールと手法を駆使してシステムへのアクセスを取得します。SQL インジェクションなどの弱点を突く場合もあれば、マルウェアやソーシャル・エンジニアリングなど別の手段を使用する場合もあります。
- **アクセス維持：**データの持ち出しや改ざん、機能の悪用など、セキュリティ侵害の潜在的な影響を実証するのに十分な長さにわたって接続を維持します。

## ペネトレーション・テスト

web アプリケーションやネットワークに侵入する方法は数え切れないほど存在し、ハッキングの手口も進化を続けています。比較的小規模な開発およびセキュリティ・チームの場合、変化のめまぐるしい最新のセキュリティ・テスト事情に精通すること、あるいはアプリケーションおよびネットワーク健全性の全体像を把握することは非常に困難です。外部のペネトレーション・テストを使用すれば、ソフトウェア開発ライフ・サイクル（SDLC）全体を通じてセキュリティ・テストを実施し、内部的なリソース不足を克服し、コンプライアンス要件を満たすことが可能となります。

ペネトレーション・テストは、企業のセキュリティにおける基盤となるもので、ハッカーと同じ視点でシステムを観察し、実際の攻撃と同じ手法やツールを使用して動作中のシステムおよびアプリケーションに存在する弱点を特定する、システムに対して許可されたシミュレーション攻撃です。SAST、SCA、脅威モデリング、アーキテクチャ・リスク分析などの手法とペネトレーション・テストを組み合わせることにより、アプリケーションとネットワークの全体像をつかむことができます。

実際の環境をシミュレーションして自動スキャンとマニュアル・テストを併用するペネトレーション・テストでは、複数の脆弱性の組み合わせによって生じる弱点を特定し、それらに優先順位を付け、最も重大なリスクを見つけることができます。これにより、開発者は悪用される前に弱点を見つけて修正することが可能となります。

## ペネトレーション・テスト・ソリューションの主な利点

### 脆弱性とセキュリティ・リスクに関する包括的なレポート

ペネトレーション・テストを実施すると、開発の最終ステージまたはデプロイ後に脆弱性を見つけて修正できます。テストはシミュレーション環境で実施されるため、業務への影響はありません。ペネトレーション・テストでシステムに存在する弱点を見つけ、既存の制御の強度を判定することにより、全体的なセキュリティ・リスクを軽減できます。

### テスト結果を実用的な形で開発チームに提供

ペネトレーション・テストは、複雑なマルチベクトル型の脆弱性などアプリケーションおよびネットワーク・サービスに存在する弱点を特定し、侵入が可能かどうかを判定します。これらのテスト結果に基づき、攻撃者によって悪用される前に開発者が問題を見つけて修正することができます。

### 低い誤検知率

自動テストと手動テストを併用するペネトレーション・テストでは、テスターが人手で結果を検証するため、高い精度が得られます。これにより、特定、検証、解決の作業に特に注意を要する高優先度の脆弱性に絞って組織のセキュリティ・リソースを集中的に投下できます。

### 開発およびテスト環境へのシームレスな統合

ペネトレーション・テスト・ソリューションは継続的インテグレーション / 継続的デリバリー（CI/CD）パイプラインの最終工程とのシームレスな統合が可能で、実行時環境を可視化します。ソースコードのエラーを特定する SAST および IAST とペネトレーション・テストを補完的に連携させることにより、ソフトウェアとシステムのセキュリティが向上します。

## 要約

**ペネトレーション・テストの利点**

- 実行時環境において包括的な診断を実施
- 複雑なマルチベクトル型の脆弱性を特定
- 誤検知率の低い高精度な結果により、トリアージが容易
- 既存の SDLC および CI/CD パイプラインへのシームレスな統合
- 実際の攻撃をシミュレーションし、悪用リスクに基づいて脆弱性に優先順位付け
- 業界規制や法的義務への準拠
- 類似アプリケーションで実績のある対策指針

## ペネトレーション・テスト・プロバイダーに求められる条件

ペネトレーション・テスト・ソリューションは多くのベンダーから提供されており、ソリューション選定の際にはいくつかの事項を検討する必要があります。どのようなソリューションを選ぶにせよ、ペネトレーション・テスト・プロバイダーは少なくとも以下の条件を満たしている必要があります。

### 経験

テスト・プロセスが文書化されていること、そして各種テスト・ツールと手法、およびユーザーが組織で使用しているプラットフォーム、アプリケーション・タイプ、およびプログラミング言語に関してチームに実地経験があることが求められます。

### セキュリティ

ペネトレーション・テスト・ソリューションは、ユーザー・データの安全を保証している必要があります。例えば、使用するセキュリティ・プロセス、アクセス・ログ（誰がデータにアクセスしたのか、など）の記録と保管方法、ユーザー・データの取り扱い方法とテスト完了後の廃棄方法などについて明確な情報提供が必要です。また、正当な権限を持つスタッフ以外にはテスト結果を開示しないことも求められます。

### コンプライアンスのサポート

PCI DSS、HIPAA、NIST、GDPR、OWASP Top 10、SANS/CEW など、ユーザー企業の事業および業界に関係するコンプライアンス基準を含め、データ・プライバシーとセキュリティに関する規制を完全にサポートしたソリューションであることが求められます。

### 自動と手動を併用したテスト・スタイル

インテグリティ・チェックやビジネス・ロジックのデータ検証などの探索的リスク解析は自動ツールで実行し、標準的なリストでは捉えきれない攻撃は手動テスト手法で調べるテスト・ソリューションが理想的です。手動テストを併用することで誤検知が抑えられ、テスト結果についてのより詳細な説明も可能となります。

### 柔軟なテスト・モデル

ペネトレーション・テストに唯一の万能なソリューションは存在しません。以下のようなツールを使用して各種テストをサポートできるテスト・プロバイダーを選ぶ必要があります。

- ネットワーク・ホストおよびオープン・ポートを検出するツール
- ネットワーク・サービス、web アプリケーション、API に対する脆弱性スキャナー
- プロキシ・ツール
- システム侵入の足がかりの取得や資産へのアクセスを実現するためのエクスプロイト・ツール
- システムとの通信、アクセスの維持と拡大、攻撃目標の達成のためのポスト・エクスプロイテーション・ツール

### 詳細なセキュリティ指針と修正アドバイス

診断で見つかった脆弱性についての関連情報や、軽減と修正のための実用的な戦略についての推奨事項を含む、詳細なカスタム・レポートを開発者とセキュリティ・チームに提供してくれるテスト・ソリューションであることが望まれます。

### 最新テクノロジーのサポート

API、マイクロサービス、サーバーレス・アーキテクチャを利用する組織が増えています。バックエンド・ロジックに潜む脆弱性を特定し、データ・フローおよび有害なデータの使用を検出・追跡できるテスト・ソリューションであることが望まれます。

### 包括的な実施条件

ペネトレーション・テスト・サービスの効果を最大限に高めるには、実施条件を定義してプロセスに対する期待値を設定し、誤解が生じないようにする必要があります。実施条件には、テスト・パラメーター、ターゲット、エスカレーション手順などの要素が含まれます。

## ペネトレーション・テスト・ソリューション・プロバイダーに確認すべき事項

- ペネトレーション・テストを実行できるアプリケーションの数に制限はあるか。
- AppSec 分野での評判はどうか。
- ユーザー自身の業界での経験があり、業界特有のニーズを理解しているか。
- 開発者サポートおよび全般的な技術サポートとしてどのようなノウハウやリソースを提供してくれるか。
- 使用しているペネトレーション・テスト・ツールはどのようなプログラミング言語、プラットフォーム、フレームワークをサポートしているか。
- ペネトレーション・テスト・ソリューションはどのような規制およびコンプライアンス基準をサポートしているか。
- ペネトレーション・テスト・ツールは組織に対する複数のエントリー・ポイントを検査してくれるか。
- ペネトレーション・テスト・ツールは従業員の意識、物理的セキュリティ、データ廃棄などのソーシャル・エンジニアリングに対応しているか。
- ペネトレーション・テストで実際にシステムへの侵害が見つかった場合、どのような対応が行われるのか。
- 実用的な対策手順を含む明確な脆弱性レポートを提供してくれるか。
- web アプリケーション、ネットワーク、API、ファット・クライアント、組み込み機器など、幅広い種類のペネトレーション・テストについての総合的な経験があるか。

## ブラック・ダックのペネトレーション・テスト

ブラック・ダックのペネトレーション・テストは、ネットワーク、API、ファット・クライアント、組み込み機器を含め、動作中の web アプリケーションや web サービスに存在する重大な脆弱性を、ソースコードへのアクセスなしに徹底的かつ体系的な方法で特定し、除去します。マネージド・ペネトレーション・テストは深度を選ぶことができ、テスト対象のアプリケーションごとのリスク・プロファイルに応じてテスト・レベルを調整できます。テスト・サービス・プロバイダーとして 20 年以上の経験があるブラック・ダックは、ペネトレーション・テストについても改良を重ねたきめ細かな実施手順書を作成しています。ブラック・ダックのエキスパートがテストを実施することにより、社内のセキュリティ・チームはより戦略的なセキュリティ目標に専念できます。ブラック・ダックのペネトレーション・テストには以下の特色があります。

- **柔軟性：**診断内容、スケジュール設定、テストの深度を管理できます。
- **一貫性：**あらゆるアプリケーションについて、同じ高品質なテスト結果が得られます。
- **網羅性：**人手によるアプローチとツール・ベースのアプローチを併用することで、徹底した結果分析、詳細なレポートの作成、実践的な対策指針の提供を可能にしています。
- **実用性：**開発者に具体的な対策指針が示されます。

組織におけるアプリケーション・テストとセキュリティの成熟度にかかわらず、ブラック・ダックのペネトレーション・テストをお受けいただくことにより、数多くの利点がもたらされます。

- 複雑なマルチベクトル型の攻撃に対する理想的な保護手段を提供します。
- 実行時の脆弱性を特定し、侵入が可能かどうかを判定することで、情報漏えいのリスクを軽減します。
- テスト結果について説明し、個々のニーズに最適な修正計画の作成を支援します。

ハッカーが見つけるよりも早く、ブラック・ダックのペネトレーション・テストが脆弱性を見つけます。

無料相談のお申し込みはこちら

# 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