参考：

[ペネトレーションテスト(侵入テスト)とは?脆弱性診断との違いや方法をわかりやすく解説｜サイバーディフェンス研究所 (cyberdefense.jp)](https://www.cyberdefense.jp/column/about_pentest.html#:~:text=%E3%83%9A%E3%83%8D%E3%83%88%E3%83%AC%E3%83%BC%E3%82%B7%E3%83%A7%E3%83%B3,%E3%82%B9%E3%83%88%E3%81%AE%E3%81%93%E3%81%A8%E3%81%A7%E3%81%99%E3%80%82)

[什么是渗透测试？ | IBM](https://www.ibm.com/cn-zh/topics/penetration-testing)

１、ペネトレーションテスト

ペネトレーションテストとはサイバーセキュリティの評価手法の一つで、セキュリティエンジニアが実際の攻撃者と同様の手法を用いて組織の情報システムに侵入を試みることでそのシステムの攻撃耐性を検証するテスト。

２、ペネトレーションテストと脆弱性診断

どちらもセキュリティを評価する手法だが、アプローチが違う。

・ペネトレーションテストは攻撃者の視点からシステムに侵入し、実際の攻撃を模擬して特定の目標達成の可否を検証するためのテストです。リアルな攻撃シナリオに基づいて侵入を試行する。

・脆弱性診断は、スキャンツールや手動によりシステム内に存在する潜在的な脆弱性を洗い出し、それらの深刻度を評価する手法

目的：

システムに対して擬似的な攻撃を行うことにより、その目標を達成可能かどうかを検証すること

３、ペネトレーションテストの種類

内部テスト（Internal Penetration Test）

外部テスト（External Penetration Test）

ホワイトボックステスト：

ホワイトボックス型のペネトレーションテストは、ペネトレーションテスターがネットワーク構成、システム内部の構造にアクセスできるため、非常に詳細な洞察が可能

ブラックボックステスト：

ブラックボックス型のペネトレーションテストは、ペネトレーションテスターが被監査組織からシステムの詳細な情報を提供されること無く、攻撃を模擬

４、課題：

コストが予測しづらい

障害発生が発生しやすいため、事前計画が入念に準備する必要がある

実施者のスキルに依存：侵入を試みるため実施者のスキルによってテストの成果が大きく変わる

５、ペネトレーションテストの主な流れ

Step1. ヒアリング

Step2. 契約手続き

Step3. 診断準備

Step4. 診断の実施

→攻撃

→脆弱性発見後にそれを起点にしてさらに別のところに侵入（踏み台攻撃など）

Step5. 報告書の提出

６、いつ実施する？

新しいシステムの導入前

システム変更後

新しいセキュリティポリシーの導入後

セキュリティインシデントの発生後

７、ほかの脆弱試験手法

TLPT(Threat Led Penetration Test：脅威ベースのペネトレーションテスト)：擬似攻撃を行うレッドチーム、攻撃に対応するブルーチームといった役割ごとのチームに分かれて攻撃シナリオをシミュレーションすることで組織の防衛態勢の評価が可能

BAS（Breach and Attack Simulation）：

BASとは実際にハッカーが行う攻撃パターンを想定し、様々なセキュリティリスクを分析できる自動化されたセキュリティ診断システム

８、おすすめツール

Metasploit

Nmap

Wireshark

９、気になるところ

実際の現場だとペネトレーションテストの使用頻度はどれぐらい？

個人的には一番聞くのは脆弱性診断。