SERVICE LINE UP

脆弱性診断

Webアプリケーションやプラットフォームに潜む脆弱性を洗い出します。

Webアプリケーションの脆弱性を点検する

Webアプリケーションの「改ざん」「情報漏えい」対策はできてますか？

設計ミスや考慮不足に伴う脆弱性がサイバー攻撃の標的となります。
ユーザーの大切な情報を守るために、典型的な攻撃パターンへの備えが重要です。

「脆弱性診断」で解決！

- ECサイトやコーポレートサイトの安全性を評価したい
- 脆弱性の診断方法がわからない
- 脆弱性診断の時間が確保できない

Service Menu **Webアプリケーション診断**

- 情報漏えい、改ざん、不正アクセス等につながる脆弱性を発見
- 発生頻度やリスクが高いサイバー攻撃への耐性を重点的に検証

ブラックボックス診断

サイバー攻撃を模した
実機によるテスト

ホワイトボックス診断

ソースコードや仕様書上の
内部構造や実装方法をチェック

診断内容の例

・各種インジェクション攻撃の実行可否　・クロスサイトスクリプティングの実行可否　・認証機能の不備
・アクセス制御の不備　・不完全な認証／認可　・セキュリティ設定の不備　・機密／機微な情報の流出可能性

ペネトレーションテスト* でサイバー攻撃耐性を評価する

＊ ペネトレーションテスト：システムに実践的な攻撃を試み、サイバー攻撃耐性を評価するテスト手法

そのセキュリティ対策、実は「抜け穴」があるかも？

抜け穴の発見には実際の攻撃を想定したペネトレーションテストがおすすめ。
システム上の課題や、サイバー攻撃によるリアルな被害が確認できます。

「脆弱性診断」で解決！

- 攻撃シナリオ作成やテストを行うスキルがない
- テストの時間が確保できない

Service Menu **ペネトレーションテスト**

- 専門の診断員がテストのすべての工程を代行
  ①攻撃シナリオの作成　②システム侵入テストの実施　③運用体制やフロー上の脆弱性を検証
  ④リスクの評価／改善策の提案

PCやサーバーの脆弱性を点検する

一台のパッチ適用漏れが命取りに！？

ウイルスへの感染や侵入を予防する日々の地道なセキュリティ対策。
これらは時に対応が漏れたり、放置されることも珍しくありません。

「脆弱性診断」で解決！

- デバイスの台数が多く、パッチ適用漏れが心配
- 定期的に診断を行いたい

Service Menu **プラットフォーム診断**

- PCやサーバーのセキュリティ対策状況を診断
  ・パッチ適用状況の確認　・ポートスキャンの実施