2. 脆弱性診断サービス

- 2.0脆弱性診断目的・スコープ・計画確認
- 2.1Web脆弱性診断
  - 自動スキャナ診断
  - 手動診断
- 2.2プラットフォーム脆弱性診断
  - サーバー脆弱性診断
  - クライアント脆弱性診断
    - PC/クライアント脆弱性診断
    - モバイル脆弱性診断
    - 多機能端末脆弱性診断
  - ネットワーク脆弱性診断
    - 無線LAN脆弱性診断
- 2.3ペネトレーションテスト
  - （Social　Engineeringによる偵察）
  - Web脆弱性診断結果からの拡張
  - プラットフォーム脆弱性からの拡張
  - 脆弱性に対する疑似攻撃（exploit）
- 2.4標的型メール対応診断
  - 入口脆弱性診断
  - 出口脆弱性診断
  - 管理レベル脆弱性診断
    - 訓練メール診断
- 2.5DB脆弱性調査・診断
  - DBアクセス経路
    - 暗号化、ログ管理、
  - サブ・インスタンス(DB)調査
  - 不適切アカウント調査
    - 不適切アクセス権調査

脆弱性診断を最小のコストで、効率的かつ効果的に実施するためには、診断の目的を明確にし、診断対象や対象範囲（スコープ）を的確に選択する必要があります。

脆弱性としては、管理面や人為的な面もありますが、ここではハード・ソフト・ネットワーク等の技術面を中心に取扱います。

脆弱性診断は多くの場合スキャンツール等で自動診断する場合が多いのですが、ツールでは診断できないケースや、グレーゾーンの取扱いについては、経験のある専門家が手動で診断する必要があります。

本サービスでは、自動診断の後、必ず手動診断で確認し、高品質を確保しています。安価な簡易診断では手動診断を行わず、スキャン結果をそのまま報告する場合もあり要注意です。

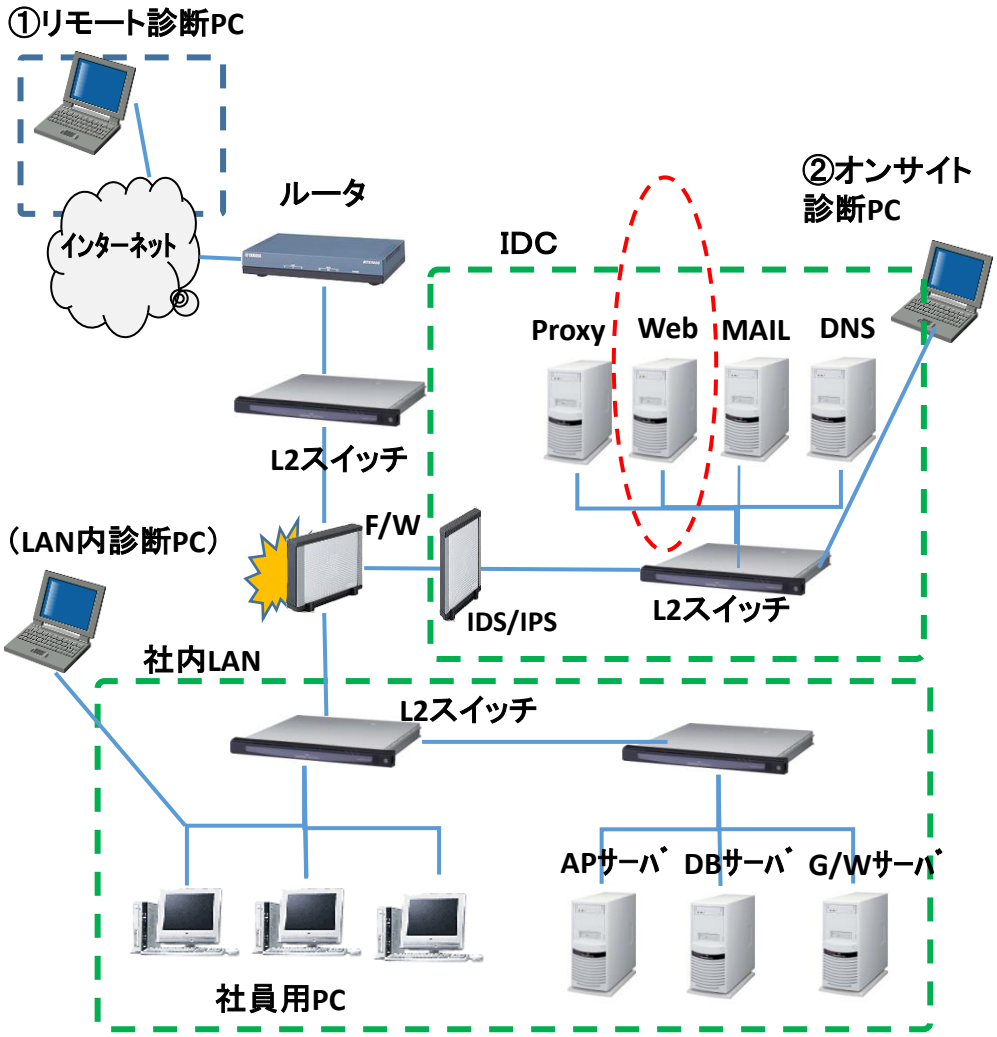
ペネトレーションは、脆弱性診断で発見された開放ポート等に対して、侵入可能な脆弱性があることを実証します。例えば、管理者権限等も奪取可能であることを示します。

ペネトレーションは専門知識が豊富な診断者が経験を駆使して、ウイルス・マルウェア・攻撃コードを想定したシナリオで、疑似侵入を実施することになります。

標的型メールでは、マルウェアが送り込まれ、外部との通信口（バックドア）を確保して、個人情報等を漏洩させます。システム的な対策の他に、利用者のセキュリティ意識レベルも評価する必要があります。

情報漏洩の視点からは、DB管理の脆弱性レベルにも注意が必要です。サーバーには、本番DBの他に、そのコピーやある条件で抽出したサブDBが多数存在しているケースが多く、それらが管理されていないケースも多々あります。これらは、アクセス権管理状況とセットで診断することが望まれます。

付2.1　Web脆弱性診断とペネトレーションテスト



・ディレクトリサーバ
・ファイルサーバ
・プリントサーバ
・メールサーバ
・Webサーバ

・DHCPサーバ
・DNSサーバ
・データベースサーバ
・アプリケーションサーバ
・仮想化サーバ
・proxyサーバ

■ペネトレーション要件確認

□Scan診断対象機器
　サーバー、F/W、ルーター、
　アプライアンス
　各種サーバー／VMマシン
　PC・・ファット／シンクライアント
　多機能端末機

・全サーバー数・・IPアドレス
・LAN接続PC数

□脆弱性診断の対象
　・Webアプリケーション
　　各種サーバー
　　DBサーバー

□ネットワーク・同機器脆弱性
　・インターネット
　・DMZ
　・社内LAN、無線LAN
　・拠点間VPN網

□診断用PC設置場所
　①リモート診断
　②オンサイト診断　DMZ
　　〃　　LAN内診断

□Webアプリ特性
　・リクエスト数
　・画面数

□脆弱性診断とPenetration Test
　・Recon
　・Mapping
　・Discovery
　・Exploit

■Webアプリ脆弱性診断

□IPAにおいて、実際に脆弱性と判断している問題

①SQLインジェクション
②OSコマンド・インジェクション
③パス名パラメータの未チェック／ディレクトリ・トラバーサル
④セッション管理の不備
⑤クロスサイト・スクリプティング
⑥CSRF（クロスサイト・リクエスト・フォージェリ）
⑦HTTPヘッダ・インジェクション
⑧メールヘッダ・インジェクション
⑨クリックジャッキング
⑩バッファオーバーフロー
⑪アクセス制御や認可制御の欠落

□OWASPが発表している2013年版の Top 10
①インジェクション
②認証とセッション管理の不備
③クロスサイトスクリプティング（XSS）
④安全でないオブジェクト直接参照
⑤セキュリティ設定のミス
⑥機密データの露出
⑦機能レベルアクセス制御の欠落）
⑧クロスサイトリクエストフォージェリ（CSRF）
⑨既知の脆弱性を持つコンポーネントの使用
⑩未検証のリダイレクトとフォワード

付2.2　Web脆弱性／プラットフォーム脆弱性診断の比較

比較項目			Web脆弱性診断	プラットフォーム脆弱性診断	備考
目的 （目的・効果に応じた最適な診断プランの作成のための明確化）			・Webページの脆弱性発見 ・APIの仕様上の欠陥発見 ‥アクセス権制御不備、管理者権限 ・APIの実装上の欠陥発見 ‥不適切なコーディング、セキュアコーディングチェック	・情報インフラの脆弱性～脅威の可視化 ・対象範囲の既知の脆弱性情報活用 ‥各種サーバ ‥OS、ミドルソフト ‥F/W、負荷分散装置 ‥thin client、fat client ・設定ミス、パッチ漏れの検出 ‥SSL/TLS、閲覧権限	・ホワイトボックステスト ‥構成情報、設定情報 ‥仕様 ・ブラックボックステスト ‥侵入目的 ‥Social Engineering
検査方法	手動検査		・事前に開発仕様を入手できると効率的 ・仕様準拠状況診断 ・誤検知は少ない	・情報インフラの構成情報の入手 ・複数ツール組み合わせ	・時間・技術者の力量
	自動検査		・仕様上の欠陥は発見困難 ・実装上の欠陥の発見に有効 ‥開発環境によるパターン化 ・誤検知の発生	・ネットワークスキャンツール ・パッチ更新もれ ・設定ミス ・手動よりも発生コスト小	・有償/無償ツール ・機械的に適用することによる誤検知発生の認識
		静的診断	・コーダーのレベルに合わせ実装工程のソースコード静的解析の継続的実施 ・APは実行しない	ー	・短時間に網羅的に実施可能 ・Jenkins等の利用
		動的診断	Webアプリケーションへの擬似的な攻撃パケットを生成し、インターネット越しに実行	ー	・短時間に網羅的に実施可能
前提			・重要性判断による実施計画 ・開発担当の協力が得られること ・AP設計情報の入手、インフラ設計情報 ・開発担当が指摘事項を理解できること	・診断の効率化のために事前情報の入手 ‥ネットワーク構成、サーバ構成、クライアント構成 ‥IPアドレス	
対策			・実装工程から継続的に診断 ・診断結果の開発者へのフィードバック	・ツール自身の定期的更新と適用	

付2.3　Web脆弱性／プラットフォーム脆弱性診断の手順

手順	お客様	NPO東京ITC	確認事項
0.事前のご相談と要件確認	診断目的・診断要件の確認	御見積書作成	目的・期待効果、診断内容 診断スケジュール、サイト規模 予算、リクエスト数の推定
	契約		診断範囲・方法・期間・場所の確認 受委託契約、守秘契約
1.診断準備	事前打合せ		診断環境確認、日程調整 診断用アカウント、IDC連絡 ネットワーク・機器構成図 診断時間帯、診断手順
	環境準備	診断計画	
2.診断実施		診断実施	診断対象範囲 診断方法‥手動/自動診断 診断場所‥リモート/オンサイト
3.診断結果分析		分析・簡易対策検討	検出課題一覧 （速報必要性）
		報告書作成	
4.報告会	報告会と問合せ対応		総評、検出課題と当面の対策 脆弱度と優先対策 再診断取扱い協議