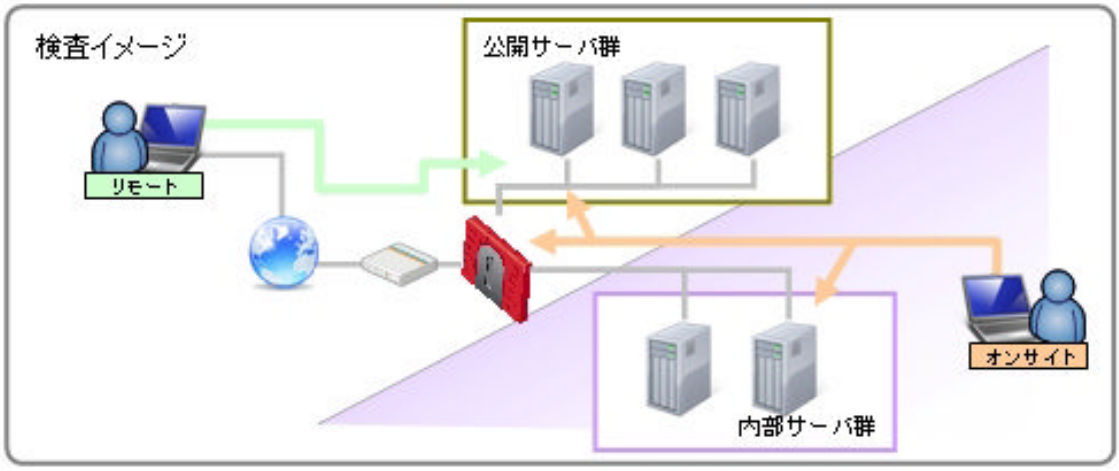
情報セキュリティ監査

ペネトレーションテスト

ペネトレーションテストとは、ネットワークに外部から不正に侵入できないかどうかを実際に試してみるテストのことです。
お客様の管理下にある情報システムに対し、内外からの不正なアクセスの可能性
（システムに潜む脆弱性）について、専門の技術スタッフが専用ツールとオペレーションにより検査を行うことです。
主なテスト項目は以下の通りです。

・外部から不正に侵入されないかどうか
・DoS 攻撃を受けた場合にどの程度耐えられるのか
・他のコンピュータを攻撃する踏み台にされないかどうか



提供している検査は以下の通りです。。
ネットワークセキュリティ検査
WEB アプリケーション検査

ネットワークセキュリティ検査

ネットワークセキュリティ検査は、お客様の管理下にあるサーバやネットワーク機器に対して、インターネット網を利用したリモートアクセスによる検査、あるいはオンサイトと呼ばれるネットワーク内部からの検査により、情報システム（オペレーティングシステム）のセキュリティ状況の確認を行い、また、それらの対策について報告するものです。

WEB アプリケーション検査

WEB アプリケーション検査は、お客様の管理下にある WEB アプリケーションに対して、
インターネット網を利用した
リモートアクセスによる検査、あるいはオンサイトと呼ばれる
ネットワーク内部からの検査により、
WEB アプリケーション特有の問題点を確認し、それらの対策について報告するものです。

検査項目例（一部です)

・クロスサイトスクリプティング
・SQL インジェクション
・セッション管理
・エラー処理
・アクセス制御
・バッファオーバーフロー　等

確認すべき項目（攻撃手法より）
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

システム及びネットワーク（設定含む）の確認すべき項目
Input Validation、入力の検証（サーバー側とクライアント側)
・SQL injection、Cross Site Scripting、HTML injection、Overflows
Access Control
・Previlege Escalation、Profile Hoping、Forceful Browsing
Password Policy（パスワードのポリシー）
・Password Strength（パスワードの長さ）、Password Resetting（パスワードのリセット）
Session Management（セッション管理）
・Session Variable Strength（セッション変数の長さ）、Session Timeout（セッションのタイムアウト）、Cookie Variables（クッキーの変数）
Security Configuration（セキュリティの構成）
・Web/Application Server（ウェブサーバー、アプリケーションサーバー）、 Lockout Account（アカウントのロックアウト）
Authentication Mechanism（認証の仕組み）
Encryption（暗号化）
・SSL、Cipher Strength（SSL の鍵の長さ）、Data Encryption（データの暗号化）
Error Messages（エラーメッセージ）
・Verbose Errors（冗長エラー）、Error Generation（エラーの生成）、Debug Information（デバッグ情報）

【ペネトレーションテスト フロー】
確認準備
対象とされるサーバ（IP 数の確認、検査方法）や Web アプリケーションで対象とする画面（画面数や遷移）について
担当者がヒアリングを行います。ヒアリングには、検査スケジュール (所要時間、業務に支障のある時間帯及び曜日の確認、テスト期間 (詳細な日時の共有は基本行いません))
緊急時の連絡先等、
手続きにおいて必要な取り決め等も含まれます。

実施
定めたスケジュールに従い、検査を実施します。
・検査の実施
・報告書の作成

報告会
検査の結果を報告書にまとめ、報告会にてご報告します。

情報セキュリティコンサルティング

ハッカー（クラッカー）は、技術的セキュリティが確保されている情報資産に対して
ネットワーク経由で攻撃をしかけてくるとは限りません。

ネットワーク管理者に近づき、だます、金品を渡す、脅すなどの
ソーシャルエンジニアリングにより、管理者権限を奪取するでしょう。

◇ソーシャルエンジニアリング　とは。

ネットワークの管理者や利用者などから、話術や盗み聞き、盗み見などの「社会的」な手段によって、パスワードなどの
セキュリティ上重要な情報を入手することです。

ペネトレーションテストで使用するツールや手法はあくまでも潜在的なセキュリティホールを発見することを目的としており、
恒常的に安全ということは保証していません。
定期的な検査の実施を推奨します。