セキュリティ診断・ペネトレーションテスト総合マップ

Ver1.1.1（最終更新：2020/05/18）

セキュリティ対策は「平常時」と「緊急時」の2つの対策に大別されます。その中で、**セキュリティ診断やペネトレーションテストは「平常時のセキュリティ対策」**に分類されます。この平常時の対策（準備や脅威の検知）をどれだけするかが、万一のインシデント発生時に対応できることに繋がるのです。

● 平常時（事前準備や脅威の検知など）

平常時のセキュリティ対策に最も重要なことは、異常発生時の検知ができることです。異常の検知ができるということは、通常どうなっているかをきちんと把握することです。具体的にはシステムの全体像を把握し、サイバー攻撃などの脅威を可視化することです。そのため、診断やペンテスト、監視等を駆使することが必要なのです。

セキュリティ対策が網羅的かつ総合的に機能しているかを可視化する

- **セキュリティ診断** ― システムを網羅的に調査
- **ペネトレーションテスト** ― 対策が機能しているか確認

JSOC

24時間365日の監視サービス

高度なセキュリティ分析システムと、セキュリティのプロフェッショナルであるセキュリティアナリストが24時間365日リアルタイムで監視・分析します。

攻撃を検知

クラウドセキュリティ設定診断

クラウド環境に特化

クラウドの課題

クラウドは変化に富んだビジネス環境に対応できる仕組みです。しかし、その反面、構築や運用の際に権限やセキュリティ設定の不備等のインシデントが発生しやすい特性を併せ持っている。

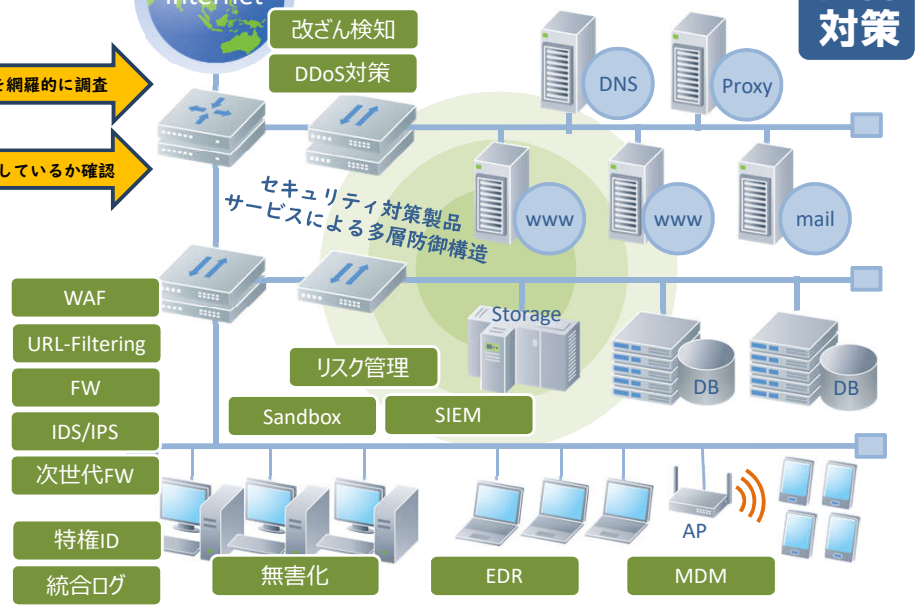
設定が適正かの管理が重要

専門家による設定確認

クラウド構築時はもちろん、運用フェーズに置いても、システムの設定変更はしばしば発生します。それらの日々の運用の中での設定が適正にされているかを、専門家がスポットおよび定期的に検証することで、お客様のシステムをセキュアに保ちます。

防御対策

攻撃者に容易に目的を達成させないために、最新の防御製品とサービスを駆使した多層防御構造の対策を実施します。



■ 緊急時（インシデント対応など）

SOCなどでサイバー攻撃などの異常を検知した際には、緊急対応フェーズへと移行します。ラックのサイバー救急センターでは、**24時間365日の対応窓口**を用意しています。最大の特徴は、**電話対応時点から経験値の高いエキスパートが実施**することです。
この体制による初動対応のスピード向上で、被害の最小化を目指します。

サイバー救急センターでの対応例

マルウェア感染	外部通報から発覚した不正侵入	クラウド環境からの情報漏洩	高度な攻撃手法による標的型攻撃

緊急対応窓口：サイバー救急センター
24時間 365日緊急対応コール
0120-362-119
ご相談は予約不要、24時間対応。すぐにご連絡下さい。
119@lac.co.jp

【サイバーセキュリティフレームワーク】

平常時

①	特定	資産管理 ビジネス環境 ガバナンス リスクアセスメント リスク管理戦略
②	防御	アクセス制御 意識向上およびトレーニング データセキュリティ 情報を保護するためのプロセス/手順 保守 保護技術
③	検知	異常とイベント 継続的なモニタリング 検知プロセス

非常時

④	対応	対応計画の作成 伝達 分析 低減 改善
⑤	復旧	復旧計画の作成 改善 伝達

出典：米国国立標準技術研究所（NIST）

【セキュリティ診断とペンテストの違い】

セキュリティ診断（脆弱性診断）はシステム全体を調査し、脆弱性や不具合を見つけるサービスです。その中で特に強く求められるのは網羅性であり、そのシステムでどのようなリスクがあるかランク付けし、一覧として報告します。一方、ペネトレーションテストは事前に作成した攻撃シナリオに沿って実施するものです。ネットワークの横展開やActive Directoryのドメイン権限の乗っ取り等が可能かどうかを検査・確認します。そのため、対象範囲が網羅的である必要性はそれほどありません。ペンテスターによる疑似攻撃が成功するか否かという点のみが重要視されます。

裏面へ

サービスメニューの詳細については裏面をご参照ください
（当社ではこの分野における各種サービスを数多く取り揃えています）

両者の違い	セキュリティ診断	ペネトレーションテスト
目的	脆弱性とセキュリティ機能の不足を網羅的に調査することでシステムの現状を把握する。	明確な攻撃の意図を持った攻撃者に、その目的を達成されてしまうかどうかを検証する
手法	各種ガイドラインなどを指標として、定型的な手法による調査を行う。	攻撃者が使用しているツール、脆弱性、ソーシャルエンジニアリング等を駆使して一定期間の検証をする。
調査対象	指定されたwebアプリケーションやIPアドレスを対象として調査を実施する。	当該組織の全体、または指定されたシステムの範囲を決めて調査を実施する。
結果	発見された脆弱性やセキュリティ機能の不足部分を一覧（項目毎にリスクの高低を記載）として提出する。	目的達成までの侵入経路や実際に行った攻撃シナリオの実施結果を提出する。

●セキュリティ診断

セキュリティ診断は、ECサイトなどのWebアプリケーション向けと組織内にあるweb、mail、DNS他のシステム基盤向けに大別されます。さらに、PC以外のデバイスなどの個別の対象にしたものを加えることが可能です。このサービスを受けることで、実施されているセキュリティ対策が有効に機能しているかを網羅的に調査します。

Webアプリケーション診断サービス

Webサイトに潜むセキュリティ上の問題点（脆弱性）を調査・検査するサービスです。この診断を受けることで、web脆弱性を介した情報漏洩などの重大事件の防止やサービス停止リスクの低減させるための提言を実施します。

Webアプリケーション診断サービス アドバンスト診断　徹底的な調査

【事前調査】あり　【診断期間】2週間～（10画面の場合の例）
【診断対象】お客様の指定した画面数すべてが診断対象
市販の自動診断ツールでは見つからない脆弱性や、脆弱性の判定が困難な脆弱性をセキュリティ専門家が**Webアプリケーションを徹底的に診断**します。

Webアプリケーション診断サービス ハイブリッド診断　バランス重視

【事前調査】あり　【診断期間】3日間～（10画面の場合の例）
【診断対象】お客様の指定した画面数すべてが診断対象
弊社独自開発のツールと専門家のスキルが必要な診断を対象用途により使い分けることで実現する、**品質と価格のバランスが取れたメニュー**です。

Webアプリケーション診断サービス ハイブリッド診断（ライトパック）　スピード重視

【事前調査】なし　診断期間】1～2日間（10画面の場合の例）
【診断対象】弊社が指定した画面（3～4画面程度）
webサイトの現状把握を最優先で実施したい、**スピード重視のお客様向け**のメニューです。調査の結果は、最短5営業日で報告可能です。

プラットフォーム診断サービス

攻撃者視点から侵入シナリオを考察し、実行することでお客様のシステムのOSやミドルウェア等で構成される**システム基盤のリスクを可視化**します。修正パッチの適応有無や推測されやすいパスワード、各種の設定不備等を確認します。

プラットフォーム診断サービス アドバンスト診断　徹底的な調査

【対象ポート】TCP:1～65535／UDP:1～1023＋主要ポート1500
【診断ツール】市販・独自ツール＋セキュリティ専門家の調査
ラックの誇るセキュリティ専門家が検出された問題を各種ツールを駆使し、複合的な調査をすることで、**システム基盤の安全度を徹底的に診断**します。

プラットフォーム診断サービス スタンダード診断　バランス重視

【対象ポート】TCP/UDP共に1～1023＋主要ポート（1400/150）
【診断ツール】市販・独自ツール
市販の診断ツールと独自開発した診断ツールを組合せることで、コストを抑えながら、詳細な診断ができます。**（HTTP、HTTPS、SMTPの重点的な診断）**

プラットフォーム診断サービス エクスプレス診断　スピード重視

【対象ポート】TCP/UDP共に主要ポートのみ（1900/180ポート）
【診断ツール】市販ツール（Qualys Guard）のみ
エキスプレス診断は、**範囲を限定、低価格でスピード感を重視**したメニューです。診断と報告書作成の4日間で診断結果を確認できます。

スマートフォンアプリケーション診断

スマートフォン環境に特化したセキュリティ診断です。以下のような脅威の状況確認を実施することで、適正な構造や設定かどうかを確認します。

❶ サーバとの通信における脅威（暗号化強度や証明書運用等）
❷ アプリケーション解析における脅威（逆コンパイル耐性等）
❸ アプリケーション操作上における脅威（パスワード取扱い等）

アジアンリンク　Webアプリケーション診断サービス SCUVA（およびSCUVA＋）　アジアンリンクの診断サービス

Web全画面へのツールによる自動診断とアジアンリンク社のエンジニアよるサンプリング診断による複合診断です。「SCUVA」は3日間限定のベストエフォート型とカスタマイズが可能な「SCUVA+」があります。

Webアプリケーション診断とプラットフォーム診断の違い

両者の違いは、診断対象の違いです。外部へ公開するwebサービスかmailサーバ等の社内システムが対象かと情報の重要度で最適なものをご選択頂けます。

Webアプリケーション診断の対象となる主なサイト	プラットフォーム診断の対象となる主なシステム
・ショッピングサイト ・会員制サイト ・検索機能を有するサイト ・社内向け業務管理サイト ・お申し込み・アンケート受付サイト ・スマートフォン・モバイル向けサイト ・Web API　・その他（動的なサイト全般）	・Web、Mailサーバ、FWなどの公開システム ・ファイル共有サーバなどの社内システム ・開発・運用ベンダのみがアクセス可能なステージングサーバ

●ペネトレーションテスト

ペネトレーションテストは、セキュリティ対策が総合的に機能しているかの確認ができます。これにより、そのシステムやサイトにおける技術的に弱い箇所やプロセス的に問題がある個所を浮き彫りにすることができます。

ペネトレーションテストサービス

ラックのペネトレーションテストサービスは、実際に悪用される攻撃手法を用いて、**システム全体への疑似攻撃**を行い、以下の4項目の観点から調査をします。

❶ ネットワーク経由での外部からの侵入
❷標的型メールによる端末感染
❸感染端末から組織内へ議事攻撃
❸検索サイト等を利用した情報収集

デバイスペンテストサービス　車載器 IoT向け

デバイスペンテストサービスは、車載器、ネットワーク機器等のIoTのペネトレーションテストサービスです。特に車載器分野は、**自動車/車載器メーカー**で多くの実績があります。

情報システム環境ペネトレーションサービス　標的型攻撃対策の確認

社内システム環境への侵入と横展開に特化したペネトレーションサービスです。**標的型攻撃などのシステムの奥深くへ侵入する攻撃への対策**状況を調査します。

TLPTペネトレーション・レッドチームサービス

TLPTは、脅威の高度化や被害範囲の見える化に対応するための「脅威ベースのペネトレーションテスト」です。国内では金融庁での方針の下、金融機関で要望が高まっています。

簡易ペネトレーションテストサービス　スピード重視

深刻な被害を伴う攻撃　のランキング上位の攻撃手法に特化したサービスです。自動検証の仕組みにより一般的なペネトレーションテストより廉価かつ短期間で実施できます。

レッドチームテクノロジーズ　Synackクラウドソーシング（CPT/CCT）

ハッキングバウンティ（報奨金）制度を背景にした50～100名の優秀なホワイトハッカーチームによるペネトレーションテストとSynackによる脅威の可視化で構成される複合的なサービスです。高スキルのホワイトハッカーの本気の疑似攻撃で調査できる事、年間契約の場合に大規模サイトでのセキュリティコスト削減などの特徴があります。

【CPT】24時間×1週間のスポットテストを中心とした短期間サービス
【CCT】CPT×2回を含んだ年間契約の総合サービス

●クラウドセキュリティ設定診断

新サービス（2020年5月リリース）　CIS準拠

近年、クラウド環境で発生するインシデントのほとんどはクラウド自体の脆弱性ではなく、構築・運用における設定ミス等によるものです。脆弱なクラウド利用で事故を避けるために専門家が診断します。

クラウドセキュリティ設定診断 by MVISION Cloud　年間サービス

McAfee社の「MVISION Cloud」導入し、お客様のクラウド環境（対応クラウド：AWS、Azure、GCP）が適切な設定になっているかを常時可視化と年4回の定期診断付きの年間サービスです。

クラウドセキュリティ設定診断　スポット診断

クラウド脆弱性をスキャナー「Nessus」を用いた、クラウド環境（対応クラウド：AWS、Azure）の設定が適正に成されているかを確認し、診断レポートをご提出いたします。

CISとは？　米国国家安全保障局（NSA）等の米国の公的機関や情報セキュリティ専門企業等が共同で研究し、米国のセキュリティ専門団体であるSANS Instituteが取りまとめたガイドラインです。

●その他（関連するサービス群）

セキュリティ診断やペネトレーションテストに関連するものや組み合わせることでより大きなメリットが得られる可能性の高いサービス群です。標的型攻撃の訓練、特定の業界や業務に特化した分野などのサービスなどがあります。

ITセキュリティ予防接種 標準サービス/セルフサービス　メール訓練

標的型攻撃等でも攻撃の初期に配信されるメール攻撃への訓練サービスです。訓練全般をラックが主導するものとツール提供のみのセルフの2種類あります。

オンライン不正・チート対策サービス　ゲーム業界 金融機関

金融系のスマートフォンアプリやオンラインゲームに特化したチート等と呼ばれる不正な利用によるビジネス運営リスクを低減させるための対策サービスです。

IoTシステム構築コンサルティング　IoTセキュリティ

IoT機器自体やIoTを含むサービス開発の際に必要なセキュリティ要件定義やセキュリティ設計、セキュア実装コンサルティングによる総合的なサービスです。

セキュリティ診断内製化サービス

Rapid7、Qualys、Vex等のツール類の導入と各種教育、アドバイザリーサポート等でお客様の内部リソースでセキュリティ診断の実施を支援するサービスです。

オンラインサービス不正ユーザ監視サービス　ゲーム業界 金融機関

オンラインゲーム等の不正をアノマリー検知（通常時と異なるプロトコルや通信先の場合にアラートを出して検知する方式）で監視するサービスです。

サーバー/クライアント端末セキュリティ設定診断　CIS準拠

サーバー及びクライアント端末環境に各種設定を解析し、現状の評価、リスク及びベストプラクティスの提示を行います。PF診断と異なり管理者権限から設定情報が適正かを診断します。

株式会社ラック　〒102-0093　東京都千代田区平河町2-16-1　平河町森タワー　|　E-Mail：sales@lac.co.jp　|　https://www.lac.co.jp/