

審査・監査

セキュリティ監査



株式会社レオンテクノロジー



デジタル社会に「安心」「安全」「安定」を

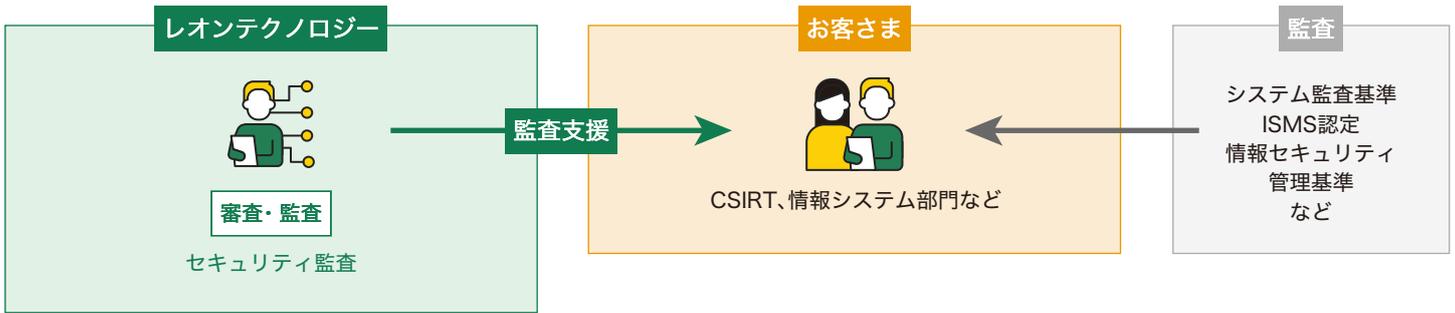
セキュリティ監査について

セキュリティ監査は、組織の情報資産を保護するために、人的、物理的、技術的な視点からセキュリティ対策の脆弱性を評価し、リスクを特定します。

セキュリティの脆弱性は、システムの技術的な弱点だけでなく、人的な運用ミスや悪意のある行為によっても引き起こされることもあります。

弊社では、独立した第三者として、情報セキュリティ監査及びシステム監査を実施します。

組織の情報セキュリティが効果的に管理され、適切に機能しているかを確認し、情報システムおよび情報資産に関するリスクについて、弊社の経験豊富な専門家が客観的に評価・助言を行います。



セキュリティ監査の必要性

本来、総合的なセキュリティ監査を定期的実施すべきですが、実際にはセキュリティ監査についての明確な指針がない組織も多く、その結果、セキュリティ監査の実施が行われないケースがほとんどです。

☑ サイバー攻撃の増加

小規模企業から大企業まで、業界を問わず多くの組織が攻撃の標的になっています。特に情報が豊富で脆弱性がある組織は攻撃を受けやすいです。

☑ データ漏えいの危険性

従業員による過誤や悪意のある行動もデータ漏えいの一因となり得ます。十分な教育やアクセス制御が不足している場合、リスクは高まります。

弊社のセキュリティ監査の特長

1



セキュリティ監査の豊富な実績とノウハウ

弊社はこれまで規模や業種に関係なく、さまざまな業界の企業に対してサイバーセキュリティに関する幅広いサポート実績を積み重ねてきました。セキュリティベンダーとしての知見もあり、包括的にご支援が可能です。

2



攻撃者の視点からのサポートができる

弊社のセキュリティ監査は、攻撃者の視点から見たセキュリティ対策の評価を行います。そのため、単なる規制順守だけでなく、実際のセキュリティ強化にも役立つサポートを提供します。

ポイント

経営層の戦略的意思決定のサポートします

経営層には、セキュリティポリシーの策定、リスク管理、組織的対応のリードなど、より戦略的な視角からのセキュリティ管理が求められます。最新のサイバーセキュリティトレンドの把握や、セキュリティに関する戦略的な意思決定をサポートする情報を提供します。

弊社が提供するセキュリティ監査の強み

お客様の独自の課題に焦点

- 情報資産に対するマネジメントを監査
- 弊社は、単に規定に従う監査だけでなく、お客様の現在のセキュリティ状況と理想状態との差を特定し、ビジネスの環境やニーズに合わせて支援を行います。一般的な解決策を提供するのではなく、**お客様の独自の課題に焦点を当てます。**セキュリティの強度に加えて、組織の情報資産に対するリスクマネジメントがどの程度効果的に行われているかの監査が行えます。

実施フロー

1

監査内容の決定

資料の閲覧やヒアリング内容をもとに監査目的や監査対象、監査範囲など決定します。

2

監査計画の作成

監査の実施内容などを示した監査計画書を作成し、具体的なスケジュールや監査手続きとご協力いただく内容を含め決定、お知らせいたします。

3

予備調査

資料の有無、内容や監査対象部門へのヒアリングを踏まえ、監査対象の概要を調査いたします。
本調査で調査・確認すべき項目の選別を行います。

4

本調査

監査計画に基づき以下のような方法で調査を行います。

ドキュメントチェック
チェックリスト精査
インタビュー
現地調査 など

5

報告書作成

予備調査、本調査にて収集した監査証拠を評価し、以下のような項目を記載したシステム監査報告書(案)を作成します。

指摘 / 改善事項
改善案

6

意見交換会報告会

監査報告書(案)を基に意見交換会を通じて事実の認識有りかなどの確認を行います。
監査報告書の最終版を作成し監査結果として報告いたします。

※製品の仕様は、予告なく変更する場合があります。なお、ご不明な場合は、当社担当営業にお問い合わせください。

※本カタログ中の情報は、カタログ作成時点のものであります。

当サービスについて詳しい内容・お問い合わせはこちらまで



株式会社レオンテクノロジー
TEL 03-5957-1960

営業時間 平日 10:00 ~ 19:00

<https://www.leon-tec.co.jp/>

本カタログのサービスの詳細情報

<https://www.leon-tec.co.jp/service/>

