

# 情報セキュリティリスク評価サービス

情報セキュリティ対策の現状レベルやリスクを各種第三者基準で客観的に評価する

## 情報セキュリティ対策の課題

情報セキュリティ対策を強化あるいは取組を開始されるお客様にとっては「どこから着手していくべきなのか」あるいは「取り組むべき対策に抜けや洩れはないのか」など判断の難しい課題が存在しています。これらを適切に解決するためには、現状のセキュリティ対策状況を調査・把握したうえで優先度を判断することが重要です。

## 情報セキュリティリスク評価サービスの概要

本サービスは、当社の専門コンサルタントが技術面・運用面・物理面において、現状の対策状況を網羅的に調査・評価し、影響の大きいリスク、優先順位、その対策方法を、専門家として客観的に報告・提言するサービスです。

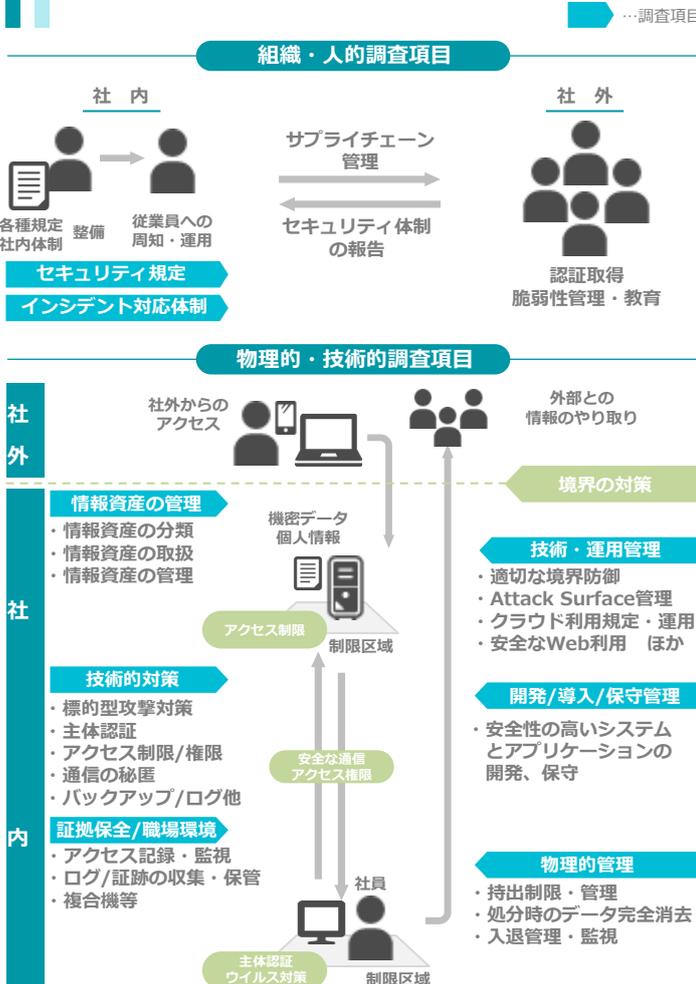
### 100項目以上の網羅的な調査

- 規定など組織的対策の評価
- IT分野の技術的対策の評価
- 建物など物理的対策の評価

### 可視化された調査報告書

- 総合評価
- 潜在リスク
- 対策案
- 現状レベル
- 要改善項目
- 個別コメント

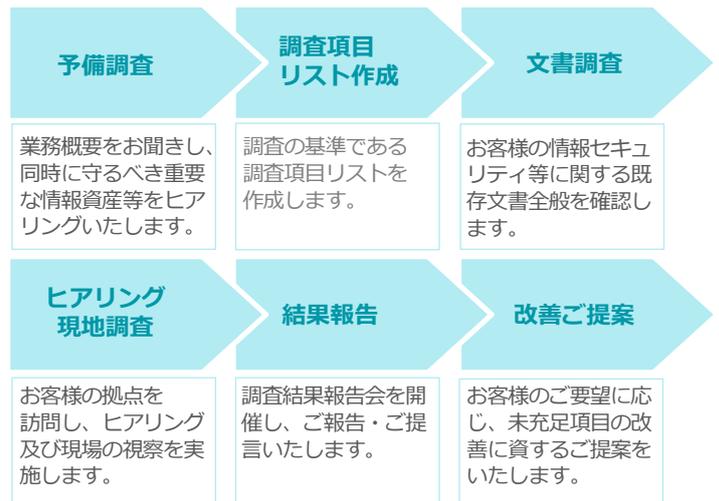
## 調査概要



## 評価基準・調査期間

評価基準	IPAセキュリティガイドライン、サイバーセキュリティ経営ガイドライン（経産省）、政府機関等の対策基準策定のためのガイドライン（内閣府）、ISMS等をベースに評価します
調査手法	調査票を元にしたヒアリング調査 各種ドキュメント・規定類の実地調査
調査期間	1か月～3か月（企業規模・診断範囲により変動）

## 実施フロー



## 報告内容の例

整理した調査結果について、リスクごとに評価をします。評価結果について、貴社と確認・検討のうえ確定し、中間報告をします。検出した脆弱性については、危険度を高・中・低の3段階で記載をいたします。

調査結果 総合評価	調査により判明したポイントを危険度に応じ3段階で評価します。
調査結果 リスク別評価	サイバー攻撃や内部不正対策、運用面などリスク別に評価します。
セキュリティ 分野別状況	情報セキュリティに対する組織的取組、運用管理、インシデントレスポンス体制など分野別に評価します。
要改善項目	相対的にセキュリティ対策が未充足と評価される項目について改善提案いたします。
情報セキュリティ 改善提案	お客様のご要望に応じ未充足項目の改善に資するご提案を別途いたします。