HITACHI
Inspire the Next

# サイバーレジリエンス対応アセスメント

サイバーレジリエンスとは、サイバー攻撃の被害が発生しても抵抗力や回復力（レジリエンス）を高めることで、事業継続を可能にする考え方、手法です。「サイバー攻撃を受ける」ことを前提とし、単なるセキュリティ対策ではなく、事業への影響を局所化することをめざします。
企業のDX（デジタル・トランスフォーメーション）が加速する一方、ランサムウェアに代表されるサイバー攻撃により、企業やサプライチェーン全体の経営が脅かされている今、事業継続のためにはサイバーレジリエンスの強化が重要となっています。

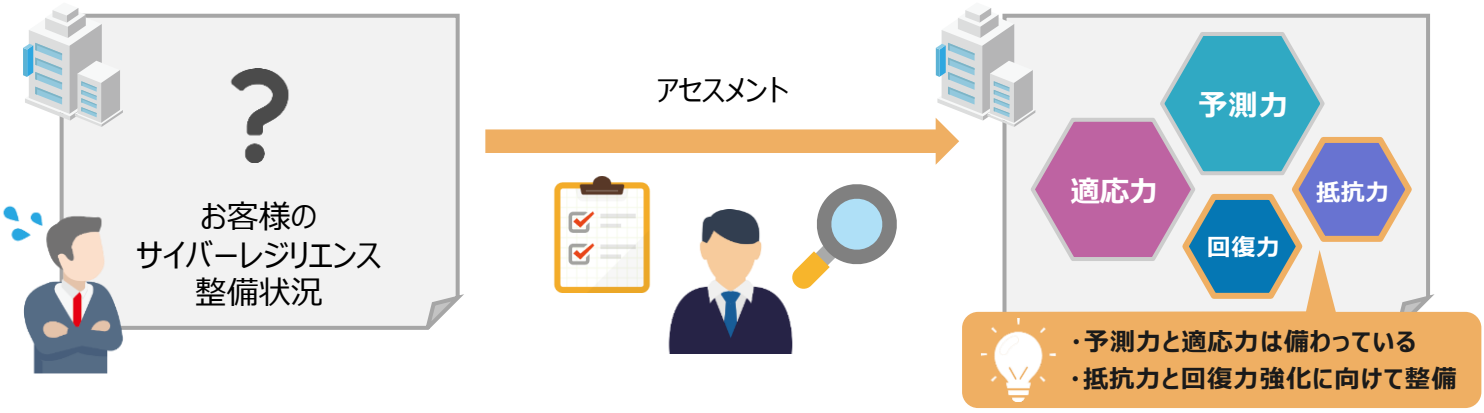
## サイバーレジリエンスを強化するため必要となる４つの力

サイバーレジリエンスを強化するために企業が備えるべきものとして、NIST（米国国立標準技術研究所）SP800-160 Vol.2では、予測力、抵抗力、回復力、適応力の4つの力を定義しています。

| 対応する力 | サイバー攻撃への対応 |
|---|---|
| 予測力 | 脆弱性・脅威情報にもとづき、準備と態勢維持 |
| 抵抗力 | 被害を局所化・最小化して事業継続 |
| 回復力 | 被害を受けても事業を素早く回復 |
| 適応力 | 技術、組織、脅威の変化を予測し事業継続に対応 |


## サイバーレジリエンス整備状況の分析

サイバーレジリエンスを強化するためにはまず、お客様のサイバーレジリエンス整備状況の現状把握と分析が必要です。
そのために日立ソリューションズの「サイバーレジリエンス対応アセスメント」では、NIST SP800-160 Vol.2にもとづいて、お客様のサイバーレジリエンス整備状況を独自の観点で評価。お客様の事業・業務に合わせ、めざすべきサイバーレジリエンスの強化を支援します。

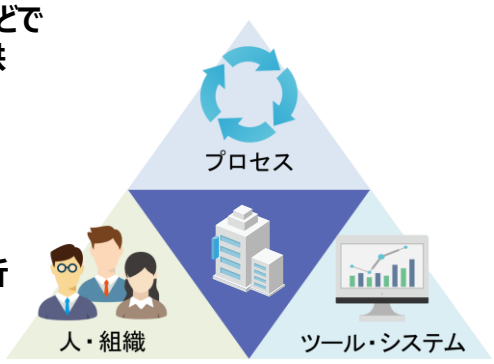



**サイバーレジリエンス強化のファーストステップとして**
**「現状把握と分析」が重要！**

株式会社 日立ソリューションズ

## サービスの特長

- **従来の情報系のアセスメントをはじめ、サイバーBCP策定コンサルティングなどで培ってきたノウハウおよび高度な知識を有するコンサルタントがサービスを提供**
- **NIST SP800-160 Vol.2をベースに４つの力の視点で、お客様のサイバーレジリエンスの整備状況を分析、報告し、対策の方向性を検討**
- **人・組織・プロセス・システム面について、４つの力にもと14項目の指標を用いてヒアリング・現場観察を実施し、サイバーレジリエンス状況を把握、分析**
- **分析結果から、お客様の現状や課題を独自手法によって明確化。セキュリティ強化ポイントを提示**




## 提供内容

- **対象システムの把握・ヒアリング調査**

対象システムの重要性やネットワーク構成など概要を把握。
サイバーレジリエンスを強化するための14のテクニックを細分化したヒアリングシートを用いて、ヒアリング調査を実施。

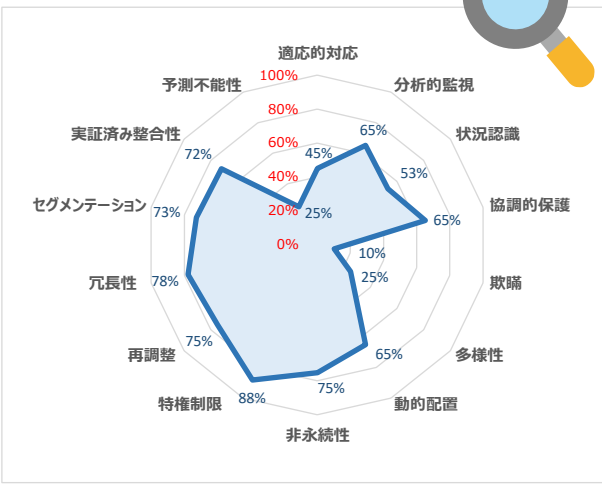
- **課題抽出・分析・対策検討**

各システムにおけるサイバーレジリエンス上の課題を抽出し、追加対策案を検討。想定されるリスクの大きさを考慮し、追加対策案の優先度を明確化。

- **報告書作成**

サイバーレジリエンスの状況について分析した結果を「アセスメント結果報告書」にてご報告。

14項目のスコア結果例




※NIST SP800-160の14項目の指標をベースに、カテゴリを分類。
各カテゴリごとに独自の観点で算出したスコアの平均値を表記。

## スケジュール

**作業期間は約1カ月から**

対象システムの把握・ヒアリング調査 ＞ 課題抽出・分析・対策検討 ＞ 報告書作成

成果物


対策状況一覧


課題への対策一覧

結果報告書



株式会社 日立ソリューションズ
www.hitachi-solutions.co.jp

本リーフレット掲載商品・サービスの詳細情報
https://www.hitachi-solutions.co.jp/security_consul/resilience_assess.html