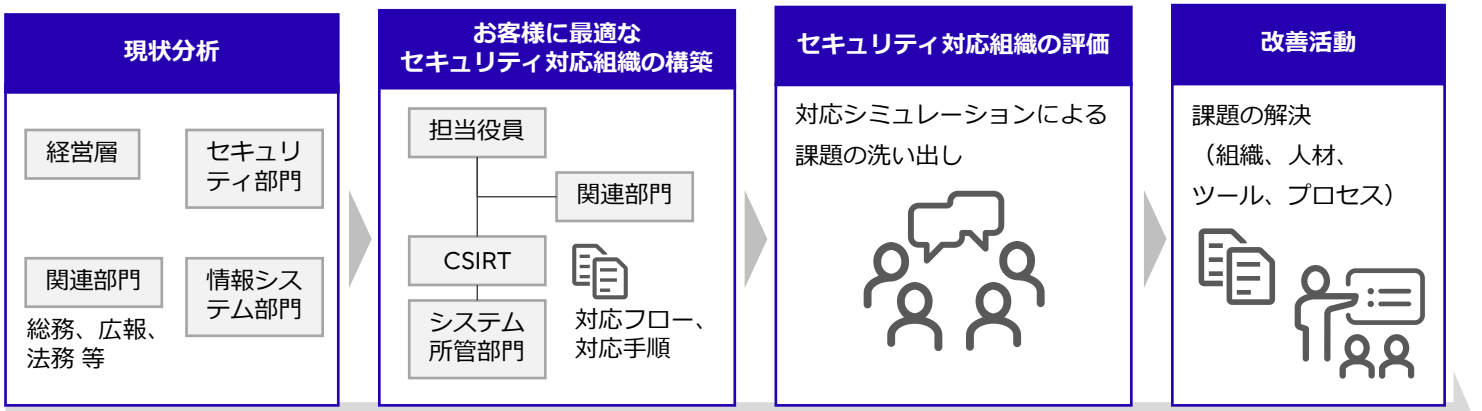
Professional Security Services

セキュリティ対応組織の強化による レジリエンス向上

多種多様な業種のお客様をご支援してきた経験豊富な富士通のセキュリティ専門家が、組織のリスクマネジメントや、最新の手法を用いて診断・評価・分析し、脆弱性がもたらす危険性と対策方針を提言するなど、お客様の課題解決やお客様自らのセキュリティ成熟度向上に向けた自走もご支援いたします。

高度化・巧妙化するサイバー攻撃を100%防ぐことは困難であり、「いかに早く検知して、被害を最小化し、業務継続・復旧できるか」というレジリエンスの向上が重要です。
富士通では、現状分析を踏まえて、「お客様に最適なセキュリティ対応組織」の構築、評価、改善活動を一気通貫で支援し、お客様のレジリエンス向上に寄与します。



（注1）レジリエンス　弾力や回復力を意味し、困難な状況に直面した際に、上手く適応したり、すぐに立ち直ったりする力のこと。

（注2）CSIRT　「Computer Security Incident Response Team」の略。
セキュリティインシデント（事件・事故）が発生した際に、中心となって対応する組織のこと。

サービスの特長

① お客様の状況を踏まえた柔軟な設計

現状を分析し、お客様に最適なセキュリティ対応組織を設計します。
また、評価や改善活動でも、お客様の目指す姿を踏まえて、最適な内容を設計します。

② 富士通知見を活かした実践的な体制強化

様々なお客様へのサービス提供から得たノウハウを活かして、実際に運用できるセキュリティ対応組織を構築します。
また、評価や改善活動でも、実際に業務で活かせる実践的な内容を提案します。

③ 一気通貫の支援

現状分析を踏まえた、お客様に最適なセキュリティ対応組織の構築から、評価、改善活動までを一気通貫で支援可能です。

サービス提供事例

現状分析を踏まえたCSIRTの構築から、評価、改善活動までを一気通貫で支援した事例です。

大手建設業様

課題 万が一 重大なインシデントが発生した場合に、対応できるか不安。

解決ポイント レジリエンス向上のために「CSIRT」を立ち上げて、継続的に評価・改善活動を実施。

1年目		2年目～
現状分析 セキュリティ対応組織として**目指す姿**と、**現状のギャップを分析**。 約1ヶ月	**CSIRT構築** 情報システム部門を中心とした**CSIRT体制を構築**。**平時の活動内容、有事の対応フローや手順**を定義。 約3ヶ月	**運用開始**（外部委託部分は当社で運用支援） **対応フローや手順の評価** **インシデント対応訓練**（ランサムウェア感染のシナリオ）によって、**検知～復旧の一連のプロセス**を**机上で確認**。 約3ヶ月 繰り返し **改善活動** ・対応フローや手順の見直し ・教育による個人のスキルアップ ・セキュリティ対策の見直し

訓練参加者の声

- 対応手順の理解が深まった。定期的に実施したい。
- 整理できているつもりだったが、具体的な行動を考えると、分からないことが多かった。
- 自分事として考えられていなかったが、心構えができた。

さらなるレジリエンス向上のために、従業員教育・訓練を実施（年1回定期的に実施）

意識向上のためのリテラシー教育

意識向上のための標的型メール攻撃訓練

サービス体系

サービス名	概要
CSIRT構築支援	セキュリティ対応組織の着実な立ち上げから、運用開始までを支援。
インシデント対応訓練	お客様環境で起こり得る有事の対応を机上シミュレーションすることで、課題の洗い出しを支援。
セキュリティ教育	お客様に最適な教育計画を立案し、教材作成から教育実施までを総合的に支援。 （従業員向けリテラシー教育、CSIRT向け教育、サイバー攻撃・対策の体験 等）
標的型メール攻撃訓練	標的型メールへの対応をシミュレーションすることで、従業員の意識向上を図る。

お問い合わせ先

富士通株式会社
富士通コンタクトライン（総合窓口）0120-933-200
受付時間：9:00～12:00および13:00～17:30（土・日・祝日・当社指定の休業日を除く）
お問い合わせフォーム