FUJITSU

サイバーインシデント対応力向上プログラム

インシデント対応体制の構築支援から、
目的に応じた教育・訓練・演習を通じて
サイバーインシデント対応力向上を実現

サイバーインシデントへの対応力向上が必要な理由

昨今、サイバー攻撃が高度化・増加していることで、防御の困難性が認識されるようになりました。よって、各組織では従来の”できるだけ防ぐ”という「防御」対策に加えて、攻撃（侵入）の発生を前提として「検知」や「対応」する力を組織として身に付けるための取り組み、すなわちSOC（Security Operation Center）/CSIRT（Computer Security Incident Response Team）の取り組みを推進しています。
SOCは外部の監視サービスを活用するケースも目立ちますが、CSIRTは様々な関連部門との調整や、ビジネス・業務への影響を考慮した対応が必要となることから自組織での運用が必要となります。

富士通総研では、お客様の状況に合わせたインシデント対応体制（CSIRT）の構築と効果的な教育･訓練･演習を通じて組織対応能力を向上させるプログラムを提供しています

サイバーインシデント対応力向上プログラムの内容

【インシデント対応体制（CSIRT）構築支援】

■ 現状を評価した上で、組織に応じたインシデント対応体制の構築を支援します

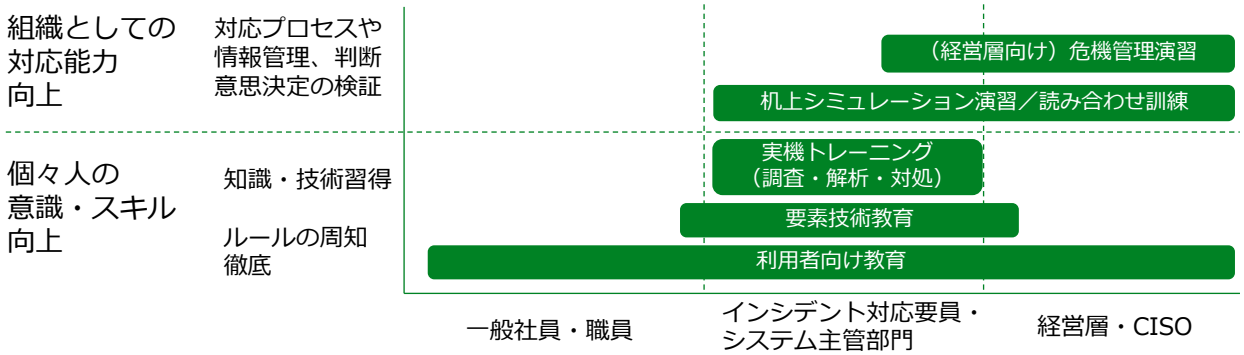
【現状評価】
- 現状のセキュリティマネジメント体制と、目指すべきCSIRT機能とのGAPを抽出し、検討すべき事項を整理
- 現状のシステム環境等を基に想定脅威を設定し、CSIRTのハンドリング対象を明確化（リスクシナリオ検討）

→

【インシデント対応マニュアル作成】
- サイバーインシデント対応に関わる役割等を定義
- インシデント対応
- マニュアル、対応フローを作成
- 残存課題を整理

【組織対応能力向上支援】

■ 専門人財育成から組織能力向上まで、目的に応じて最適な手法で対応能力の向上を支援します



サイバーインシデント対応力向上プログラム

インシデント対応体制の構築支援から、目的に応じた教育・訓練・演習を通じてサイバーインシデント対応力向上を実現

サイバーインシデント対応力向上プログラムの内容

CSIRTとしてのインシデント発生時の行動を整理した上で、必要な知識やノウハウの講義を実施。最後に、実践的な対応力を身につけるための演習を実施。

構成	内容
インシデントハンドリングマニュアル作成	• インシデント発生時のCSIRT、ならびに関係部署の行動を整理
読み合わせ訓練	• 関係部署にて、インシデント発生時の行動を整理したフローの確認を行い、修正点を抽出すると共に、インシデント時の共通認識を醸成
オリエンテーション	• 滞りなく演習を進めるためにルールを説明する（シナリオ非提示） • 演習の目的・目標を説明し、参加者に理解・浸透させることで演習実施後に達成度や課題を明確にする
机上シミュレーション演習（※）	• インシデント検知後に起こり得る状況を演出 • 参加者自らが役割に応じた対応を実施 • あるべき対応とのギャップを講師から指摘し、課題を認識
ホットウォッシュ（振り返り）	• 気づいた課題や、今後の対策を参加者で議論 • 議論した課題を見える化、共有し、当事者意識を醸成

※机上シミュレーション演習：
サイバーインシデント発生時の状況（シナリオ）を模擬的に再現することで、参加者に状況把握のための情報収集や暫定対応の検討・判断等を実践していただく演習です。

サイバーインシデント対応力向上プログラム　ご提供価格・実施期間

メニュー	価格（税別）	実施期間（目安）
インシデント対応体制（CSIRT）構築支援	300万円～	約3ヶ月～
机上シミュレーション演習	個別お見積り※	約3ヶ月～

※演習目的や手法、参加者によって価格が異なるため、個別見積させていただきます。
※本記載内容は予告なく変更する場合がございます。

株式会社富士通総研[FRI]
レジリエンストレーニングセンター（政策支援グループ内）
Tel. 03-6424-6751（代表）　Email. fri-bcm-dm@cs.jp.fujitsu.com

2022年4月現在

© 2022 FUJITSU RESEARCH INSTITUTE