本サービスは『CSIRT構築 ベストプラクティス・テンプレート』のオプションサービスです。お客様独自のインシデント対応マニュアルを利用しての訓練につきましてはご相談ください。

CSIRT構築 ベストプラクティス・テンプレート　オプションサービス

CSIRT向け インシデント対応机上訓練

情報セキュリティインシデント発生時の組織的対応を訓練

CSIRT構築 ベストプラクティス・テンプレートで構築したインシデント対応体制の即応能力を訓練する

CSIRT（Computer Security Incident Response Team）は、組織内で発生したセキュリティインシデントの対応のマネジメントを担うほか、平常時には、組織全体の情報セキュリティを向上させるための情報収集や教育などを行う組織です。近年、多くの企業・団体でCSIRTが導入されていますが、一方で導入後のCSIRT運営に苦労するといった例が少なくありません。特にCSIRTの主要機能であるインシデント対応能力の習得・向上は、平時からの訓練と訓練結果に基づくインシデント対応フローの見直しの継続に依るところが大きく、定期的な実施が有効です。しかしながら、多くの組織では実際のインシデント対応経験が無いため、訓練効果の高いシナリオの作成や訓練結果の評価について参考とすべきベストプラクティスが乏しく訓練企画が難しいという課題があります。

■ CSIRTの主な機能と訓練対象範囲

訓練範囲

	平常時のCSIRT活動		事故時のCSIRT活動
	インシデント事前対応	セキュリティ品質向上	インシデント事後対応
調査方針策定機能	☑セキュリティ関連情報収集 ☑技術動向調査 ☑脆弱性情報対応	☑セキュリティ関連情報収集 ☑技術動向調査 ☑脆弱性情報対応	☑インシデント対応 ☑インシデント対応方針策定
対応機能	☑セキュリティツールの開発	☑製品評価・認定	☑インシデントハンドリング ☑インシデント対応支援
チェック機能	☑インシデント/セキュリティイベント検知 ☑セキュリティ監査/査定	☑リスク評価・分析 ☑セキュリティリスクコンサルティング	☑インシデント/セキュリティイベント検知
教育機能	☑セキュリティ関連情報提供	☑セキュリティ教育 ☑トレーニング ☑啓発活動	
窓口機能	☑外部団体との連携	☑外部団体との連携	☑発生報告受付（社内/外部）

CSIRT向け インシデント対応机上訓練サービス 概要

机上訓練とは実際の攻撃を用いた演習とは異なり、参加者によるシナリオの読み合わせをベースとして、インシデント対応の手順を関係者間で疑似体験する訓練手法です。訓練によって対応手順上のボトルネックを明確にし、手順書の改訂を通じて組織対応力の向上につなげます。ソリトンシステムズの机上訓練サービスは独自監修の複数のシナリオからお客様の環境に最適なシナリオをご選択いただけます。訓練の準備、当日の進行、訓練により判明した課題のとりまとめ、総評レポートの作成までをソリトンシステムズが代行します。

■ 机上訓練のながれ

訓練仕様

着手より報告書納品まで概ね2か月程度のプロジェクトとなります。

	項　目	説　明
1	訓練目的	• 既存のインシデント対応手順の実効性を評価 • 対応上のボトルネックを洗い出し手順を改訂
2	訓練方法	• 会議室等に集合し、シナリオの読み合わせをベースに対応フローを確認する集合方式
3	訓練対象者	• CSIRTメンバーおよびその他社内関係者が対象
4	訓練シナリオ	• ソリトンシステムズ監修シナリオ6本より選択
5	成果物	• インシデント対応訓練報告書を納品
6	その他	• 事前準備期間：キックオフ後約１か月 • 訓練日数：1日

近年のサイバー攻撃動向を反映した訓練用ベースシナリオ

訓練用のベースシナリオは近年のサイバー攻撃動向を踏まえ、実践的な内容を加味した8本のうち１本を選択可能です。

	発生インシデント	想定する攻撃手法	想定する攻撃対象
1	Webサーバーへの不正アクセス	Webサーバーの脆弱性攻撃	Webサーバー
2	Webサーバーへの DDoS攻撃	DDoSによるサーバーリソース枯渇攻撃	Webサーバー
3	電子メールによる標的型攻撃	電子メール添付のマルウェア攻撃	組織内LAN端末
4	ランサムウェア感染	ランサムウェア攻撃	組織内LAN端末
5	サプライチェーン攻撃と金銭恐喝	サプライチェーン攻撃	組織内LAN環境
6	人的ミスによる機密情報漏えい(メール)	電子メールの誤送信	組織内LAN端末
7	人的ミスによる機密情報漏えい(Web)	Webサーバーにおける作業ミス	Webサーバー
8	内部不正による情報漏えい	内部不正	組織内LAN環境

ご利用条件

本訓練サービスはソリトンシステムズ「CSIRT構築 ベストプラクティス・テンプレート」のオプションサービスです。お客様にて独自整備されたマニュアルでの訓練につきましてはご相談ください。

インシデント対応マニュアルの種別	サービス利用
ソリトンシステムズ CSIRT構築 ベストプラクティス・テンプレートで作成したインシデント対応マニュアル	○ 訓練サービスをご利用いただけます
お客様独自作成のインシデント対応マニュアル	△ ご相談ください ※ 条件により対応できない場合があります

お問合せはこちら：**株式会社ソリトンシステムズ**　サイバーセキュリティ事業部　cyber-sales@list.soliton.co.jp／ TEL 03-6369-8015