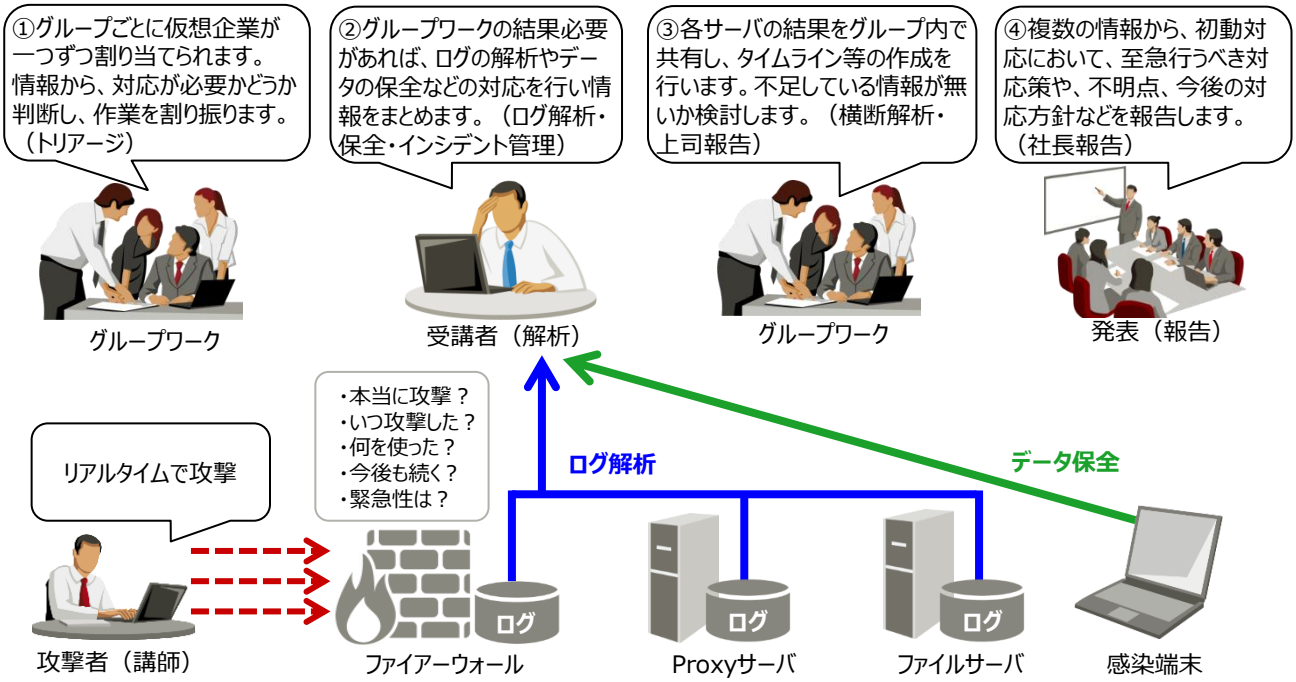
FUJITSU 人材育成・研修サービス
講習会
サイバーレンジによる実践的インシデント訓練

本コースでは、サイバー攻撃におけるインシデント対応を実践的な訓練形式で学びます。サイバーレンジ内でセキュリティインシデントが次々に発生しますので、現場で対応するSEとしてインシデントの初動対応をグループで訓練することができます。

こんな課題をお持ちの方におすすめします

- **サイバー攻撃を受けた場合の対応に不安がある方**
- **インシデント対応の経験がないので失敗できる環境で事前に訓練しておきたい方**
- **実際の業務に近い環境でインシデント対応を訓練したい方**

参考：本コースで訓練するインシデント対応のイメージ



本コースおすすめのポイント！

- **実際に動作している仮想環境でインシデント対応を訓練！**
- **1時間ごとの上司報告や最終的な社長報告など実際の業務さながらの緊迫した訓練！**
- **同時多発的に発生するリアルタイムなインシデントで実践的に訓練！**

コースの概要

サイバーレンジによる実践的インシデント訓練

期間：2日間

項目	内容
コースコード	USA60L
受講対象	一般的なシステム開発、運用を担当するSE
コース概要	システム運用の現場において、セキュリティインシデントが発生した場合、多様なOSやミドルウェア、プロダクト、ネットワーク機器やセキュリティ機器から発生する情報を収集し、セキュリティインシデントかどうかの判断が求められる。本教育は、セキュリティインシデント発生時における初動対応を実現するために、簡易的な調査や分析が行えることを確認する（実践的な内容のため講義は最小限です）。
前提知識	3年程度の運用保守の実務経験を有すること。CCNA程度のネットワークに関する知識を有すること。MCSA程度のWindowsOSに関する知識を有すること。LPIC レベル2程度のLinuxOSに関する知識を有すること。ITIL Foundation程度のITサービスに関する知識を有すること。
コース価格	250,000円 (税別)
注意事項	・本コースは「前提知識が満たされていること」を前提として開催します。各サーバのコマンド操作方法やログの閲覧方法についての講義はありません。前提知識を確認の上ご受講ください。 ・演習はグループワークです。 ・「サイバーレンジによる実践的インシデント訓練」（YAZ05L）コースをご受講済の方は、内容が重複いたしますのでご了承ください。

日程・スケジュール

時間	1日目	2日目
午前	第1章　訓練の必要性 仮想企業の組織構造とシステム構成 演習1「仮想企業に対する攻撃と対策の検討」 第2章　セキュリティインシデント対応実践 訓練の概要 演習の進め方 サイバーレンジの操作方法	演習2「初動対応の実践」（続き）
午後	演習2「初動対応の実践」	演習2「初動対応の実践」（続き） 演習3「報告の実践」 まとめ

関連コースのご案内：2018年度上期 新設コース

コースコード	USA61L
コース名	サイバー攻撃手法と攻撃検知手法
受講対象	SOC（セキュリティオペレーションセンター）のような業務を今後担当される方
コース概要	近年の攻撃者は標的およびそのシステムを綿密に調査し長期間にわたって機会をうかがって攻撃を行います。そのため、「侵入されることを前提」として、素早く検知し、対抗手段をとるかが重要です。未知の攻撃が増えている現在においては、現存の攻撃手法を知り、それを検知する実体験の積み重ねが重要です。本コースの演習ではAPT攻撃を模した攻撃演習シナリオを用いて攻撃手法および検知手法を体験し知見を得ることを目的としています。攻撃演習シナリオに沿って、攻撃者の立場で実際に企業ネットワークに模した環境に攻撃を実施し、防御側の立場で実際に攻撃の痕跡を検知します。この体験を通し、さらなるセキュリティマインド、検知/防御技術の向上に役立ててください。
期間	2日間
価格	300,000円 (税別)

お問い合わせ先

お客様総合センター

0120-55-9019

受付時間 9:00～17:30（土・日・祝祭日を除く）

株式会社富士通ラーニングメディア　〒108-0075 東京都港区港南2-13-34 NSS-IIビル　http://www.knowledgewing.com/