Internet Initiative Japan

Internet Initiative Japan Inc.
Phone 03-5205-6310 E-mail press@iij.ad.jp URL https://www.iij.ad.jp/
Address Iidabashi Grand Bloom, 2-10-2 Fujimi, Chiyoda-ku, Tokyo 102-0071, Japan

PRESS RELEASE

2021 年 12 月 20 日
株式会社インターネットイニシアティブ

IIJ、セキュリティスペシャリストを育成する独自教育プログラム「IIJセキュリティ教習所」を開設

--自社のセキュリティサービス運用やインシデント対応で培った知見をベースに実践的プログラムを提供--

当社は、セキュリティスペシャリストを育成する事業として、IIJ 独自の教育プログラム「IIJ セキュリティ教習所」を開設いたします。
IIJ セキュリティ教習所は、企業の情報システム部門のセキュリティ担当者や CSIRT(※1)部門担当者を対象に提供する教育プログラムで、IIJ セキュリティオペレーションセンター(SOC)でのインシデント対応やサービス運用で得られた知見をベースに、基礎から応用知識までを体系的に学べる研修内容となっています。実践をふまえた演習により、自社で実際にインシデントが発生した際に、セキュリティスペシャリストとして適切な判断・対処が行える人材を育成いたします。
第一弾として、2022 年 1 月より「インシデントハンドリング実践コース」を開始します。当コースは情報処理安全確保支援士(登録セキスペ)(※2)の特定講習(※3)として経済産業省令にて定められたものとなります(特定講習番号 21-007-022)。
続いて 2022 年 3 月より、「攻撃技術理解・防御 APT(※4)対策基礎コース(仮称)」を開設予定で、以降も順次プログラムを拡充してまいります。

(※1)CSIRT(シーサート):Computer Security Incident Response Team の略で、コンピュータセキュリティにかかるインシデントに対処するための組織の総称。
(※2)登録セキスペ:セキュリティに係る最新の知識・技能を備え、企業や組織のサイバーセキュリティの確保を支援する専門人材であることを示す国家資格。
(※3)特定講習:登録セキスペに受講が義務付けられている講習を民間事業者等が行うもので、IPA(情報処理推進機構)が行うサイバーセキュリティに関する講習と同等以上の効果を有する講習として、経済産業省令で定められたもの。
(※4)APT :Advanced Persistent Threat の略。特定企業のネットワークに侵入し、長期的に情報窃取や破壊活動を行うサイバー攻撃を APT 攻撃と呼ぶ。

■背景

サイバー攻撃が日々高度化するなか、政府は「サイバーセキュリティ経営ガイドライン」で、民間企業をはじめ各組織に対して、サイバー攻撃を受けた場合に備えて“緊急時の対応体制(緊急連絡先や初動対応マニュアルの整備、実践的な演習の実施)”の構築を推奨しています。一方で、企業ではセキュリティ人材やスキル不足が大きな課題となっており、セキュリティ人材育成を支援する教育サービスの需要が高まっています。特に現場での対応が求められるセキュリティエンジニア育成のため、実際に発生したセキュリティインシデントへの模擬訓練実施等、実習型プログラムへの需要が増えており、IIJ では今回、セキュリティオペレーションセンター(SOC)の最前線で培った経験とノウハウをもとに、実践力の高い知識・スキルが習得できるプログラムを提供するものです。

■IIJ セキュリティ教習所の特徴

基礎から応用、高度まで体系的なプログラムを提供
20 年以上にわたるセキュリティサービス運用や SOC でのインシデント対応で培った知見、およびこれまで社内でセキュリティアナリストを育成してきた教育実績をもとに、本当に現場で必要となる知識を“基礎”、

“応用”、“高度”に分類し、体系的に習得できるプログラムを用意します。基礎知識を習得できる基礎レベルから実用性の高い応用、特定分野に特化した高度レベルまで、必要なレベルに応じた知識・スキルを効率的に習得できます。

実践演習によりすぐに役立つ知識、スキルを習得可能

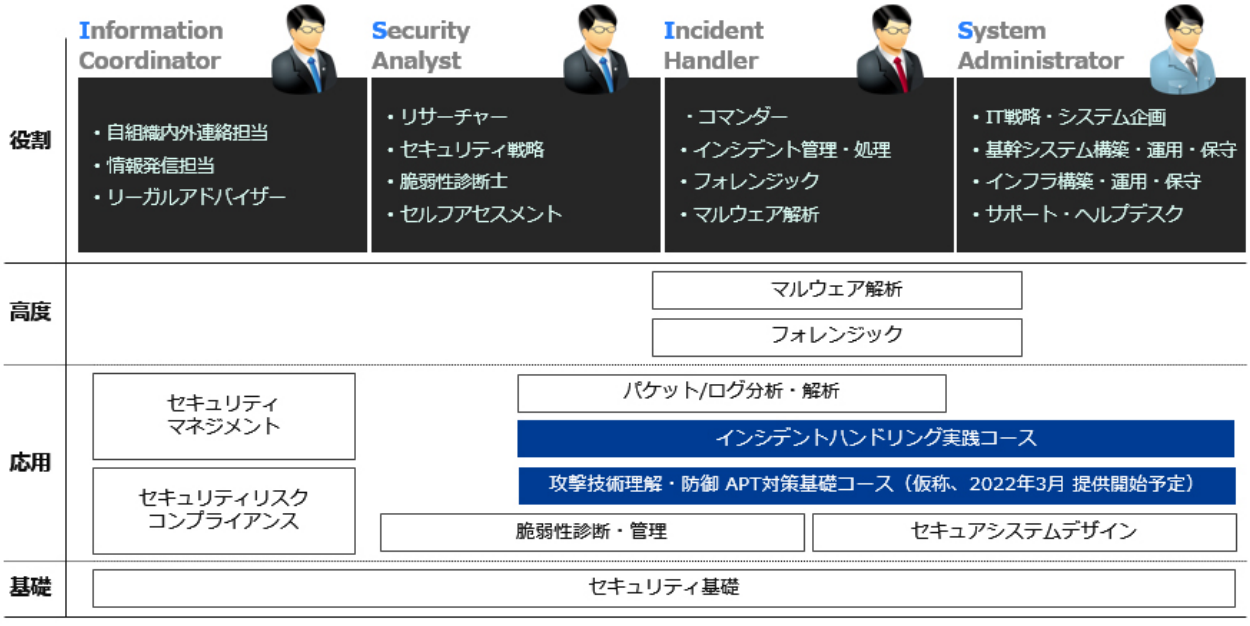
机上の座学講習だけではなく、IIJ SOC で実際に対応したインシデント事案をベースに、実践を想定した演習をすることで、実際の現場ですぐに活かせる知識・スキルを身につけることができます。ログ解析からインシデントの特定、対処といった事案対応のみならず、組織内での影響度合いの想定、報告方法など、セキュリティ部門としての適切な初動対応に必要な知識と技術を習得可能です。

現場で実際にインシデント対応をしているエンジニアによる直接講義

社内外で長くセキュリティ教育に携わった経験を持つ講師、および、実際にインシデント対応などを行っている IIJ のセキュリティエンジニアが、自らの経験を生かして講義を行います。
さらに国内外で多数の講演や講義の実績のある IIJ のセキュリティエンジニアによる講義も開催予定です。特に、Black Hat USA(※5)で日本人として初めてトレーニング講師に選ばれたエンジニアによる最高水準のセキュリティ対応技術を直接学ぶ機会の提供も予定しています。

(※5)Black Hat USA:1997 年から続く世界有数のセキュリティカンファレンスで、世界各国からセキュリティエンジニアやハッカー、研究者が参加する。

■プログラム構成概要



■プログラム概要

インシデントハンドリング実践コース

プログラム内容：1. 基礎知識講義
2. 最新セキュリティ動向講義
3. インシデントハンドリングの流れと実践(ログ解析や切り分け作業)
4. 実践内容の振り返り

習得技術：IIJ SOC で実際に対応したインシデントをもとに作成した疑似インシデントへの対応を通して、インシデント発生の連絡からクローズまでの対応方法/インシデント発生時の適切な初動対応方法といった、インシデントハンドリングに要求される知識やスキルを習得します。

研修期間:　1 日（10:00～18:00）
定員:　4 名から開催
受講価格:　80,000 円（税込）/ 人
提供開始:　2022 年 1 月

攻撃技術理解・防御 APT 対策基礎コース（仮称）

プログラム内容:
1. 基礎知識講義
2. 最新セキュリティ事例講義
3. サーバ・端末に対する攻撃手法の解説
4. 攻撃に関するログの調査・対策方法の検討

習得技術:　インシデント対応の専門家による、実際に発生した最新の攻撃手法を踏まえた演習を通して、ログの見方、セキュリティ対策の考え方/インシデント発生時の適切な初動対応方法など、実際の現場ですぐに活用できる実践的な検知・防御方法を習得します。
研修期間:　1 日（10:00～18:00）
定員:　4 名から開催
受講価格:　未定
提供開始:　2022 年 3 月

※新型コロナウイルス対策を徹底したうえで実施します。感染対策については以下のサービス詳細サイトをご覧ください。

- サービス詳細は https://www.iij.ad.jp/svcsol/security-education/ をご覧ください。

IIJ は今後も、「安全をあたりまえに」をコンセプトとするセキュリティ事業ブランド「wizSafe（ウィズセーフ）」の下に、インターネットを誰もが安心して安全に使える社会インフラへと発展させるべく、活動してまいります。

報道関係お問い合わせ先
株式会社インターネットイニシアティブ　広報部　増田、荒井
TEL:03-5205-6310　FAX:03-5205-6377
E-mail:press@iij.ad.jp　https://www.iij.ad.jp/