CTC
Challenging Tomorrow's Changes

セキュリティエンジニア養成講座

サイバーセキュリティの現状

頻発するサイバー攻撃

- 2017年上半期のサイバー犯罪相談件数は過去最大の6万9977件*1。
  セキュリティ侵害の発生から検知までに要した日数は平均172日*2。
- サイバー攻撃手法の高度化・巧妙化によりセキュリティ侵害を完璧に防ぐことは不可能。

不足するセキュリティ人材

- セキュリティ人材の不足数は13.2万人、2020年には不足数が19.3万人にまで拡大する見込み*3。
  セキュリティ知識分野（SecBoK）人材スキルマップ*4ではセキュリティ人材を16の役割に分割。
- セキュリティ人材の役割は多岐に渡り、また、実体験を通した技術習得が難しいため育成に時間が掛かる。

*1：平成29年上半期におけるサイバー空間をめぐる脅威の情勢等について｜警察庁
https://www.npa.go.jp/publications/statistics/cybersecurity/data/H29_kami_cyber_jousei.pdf
*2：M-Trends 2017 Infographic｜FireEye
https://www.fireeye.jp/content/dam/fireeye-www/regional/ja_JP/services/pdfs/ig-mtrends-apac.pdf
*3：IT人材の最新動向と将来推計に関する調査結果｜経済産業省
http://www.meti.go.jp/press/2016/06/20160610002/20160610002-7.pdf
*4：セキュリティ知識分野（SecBoK）人材スキルマップ｜JNSA
http://www.jnsa.org/result/2017/skillmap/

CTC教育サービス セキュリティエンジニア養成講座の3つの特徴

特徴 1　今、求められるセキュリティスキルを習得

攻撃者の視点でシステムの脆弱性を分析するスキルやインシデント（セキュリティ事件・事故）の発生を前提とした検知・対応スキル等、もっとも必要となるセキュリティスキルを習得することができます。

特徴 2　体験を重視した充実の演習環境

ハッキングツールを用いたサイバー攻撃やフォレンジックツールを用いたログ分析、マルウェア解析等、豊富な実機演習を通して、攻撃者の視点や被害者の立場を疑似体験できます。

特徴 3　初学者にも分かりやすい講義

初学者には敷居が高いセキュリティ技術。しかし、CTC教育サービスでは経験豊富な講師陣が分かりやすい説明を心がけて講習を行っていますので安心です。

セキュリティエンジニア養成講座のコース体系

- セキュリティエンジニア養成講座はセキュリティ対策の各フェーズ（導入⇒運用⇒インシデント対応）に対応した下記3コース（コースコード：N472、N474、N476）で構成されています。
- セキュリティエンジニア養成講座の修了条件は次の通りです。
  - 下記3コースを全て受講（受講の順序は問いません）、かつ、出席率90%以上。
    ＊複数の開催日程（年間8～10回程度）の中からお好きな日程を選んご受講いただけます。
    ＊開催日程の詳細については、弊社Webサイトでご確認ください。
  - 各コースの最後に実施する修了テストに合格。

コースコード N472　実践！セキュリティ（サイバー攻撃手法とその対策）～ハンズオンで学ぶ各種ハッキング手法～

コース概要：ハッキングツールを用いたハンズオンを通して、コンピュータネットワークにおける脅威とその対策について学習するコースです。不正アクセスやDoS/DDoS攻撃といった従来型のサイバー攻撃だけでなく、最近注目を集めている「標的型攻撃」についても取り上げ、それぞれの技術的な仕組みを学習します。また、情報セキュリティ対策の概念や、ファイアウォール（従来型/次世代）、UTM等の各種セキュリティデバイスの特徴についても学習します。

コースコード N474　実践！セキュリティ（セキュリティ運用/インシデント検知）

コース概要：セキュリティ運用（セキュリティ情報の収集やパッチ管理、各種ログ分析等）のノウハウを習得するためのコースです。日々、発見される脆弱性情報の収集方法やインシデント（セキュリティ事件）をいち早く検知するための事前準備事項、インシデント検知の観点からサーバやセキュリティデバイス（ファイアウォールやIPS、UTM等）のログを分析する手法について、座学と実機演習を通して学習します。また、本研修の最後には、被害が発生したサーバのログを分析し、攻撃手法の特定や対処方法の検討を行っていただく総合演習をご用意しています。

コースコード N476　実践！セキュリティ（インシデント対応/フォレンジック調査）

コース概要：インシデント対応（セキュリティ被害が発生した際の対処方法）に関わるノウハウを習得するためのコースです。インシデント調査の対象となるデジタルデータの適切な保全方法や、被害状況・原因を明らかにするための調査方法について、座学と実機演習を通して学習します。また、マルウェアの可能性がある不審なファイルを解析（マルウェアか否かの判別や動作・振る舞いの確認）する方法についても学習します。

CTCテクノロジー株式会社
エデュケーション企画推進部
〒154-0012 東京都世田谷区駒沢 1-16-7 駒沢中村ビル
TEL.0120-667230 ※9:00 ～ 17:30（土日・祝日・年末年始を除く）受付
FAX.0120-667235 ※24 時間受付
E-mail:kyouiku@ctc-g.co.jp
http://www.school.ctc-g.co.jp