セキュリティ技術基礎【オンライン受講のみ】（4120028）

～もう知らないでは許されない！セキュリティ技術を基礎から学ぼう～企業の情報資産を保有・管理しているIT部門は、情報セキュリティの脅威と対策を理解する必要があります。情報セキュリティの脅威と対策を本質的に理解するためには、その基礎となる技術要素を理解する必要があります。本講座では、IT担当者が直面する情報セキュリティ対策に関する基本的概念から、情報を保有する脅威と求められる対策（人的・技術的・物理的）における技術的な基礎知識を習得します。

開催日時	2021年3月2日(火) 10:00-17:00ライブ配信 2021年3月3日(水) 10:00-17:00ライブ配信
カテゴリー	共通業務（契約管理、BCP、コンプライアンス、人的資産管理、人材育成、資産管理）・セキュリティ・システム監査 専門スキル
DXリテラシー	How(データ・技術の活用)：留意点
講師	安田良明 氏 （株式会社ラック　事業統括部 担当部長 ） 1996 年 情報通信メーカーへ入社。システムズエンジニアとして、ナショナルセキュリティ分野に関する情報システム構築、 セキュリティオペレーションセンター構築を従事する傍ら、2005 年から2007 年に掛けて、米国の情報保証技術の調査研究を行う。 2009 年 株式会社ラックに入社。サイバーリスク総合研究所の研究員として，研究成果の製品化、 特定用途システムへの転用提案や情報セキュリティ教育、人財育成などを担当。 2010 年 ナショナルセキュリティセンターを設立し、初代センター長として就任。 社会システムが期待する情報保証技術の調査研究を行うと共に、国家の安全保障を担うシステムに対し、 自社の研究成果を提供し、社会セキュリティの確保に貢献する活動を行う。 2011 年 内閣官房情報セキュリティセンターセンター員として、 情報セキュリティ対策の推進に関する専門的、技術的な事項についての支援業務を行う。 2013 年 S&J株式会社へ入社。 組織の業務とITの状況を可視化し、トップダウンのガバナンスコンサルタントを行う。 インシデントが発生したお客様に対して、インシデントレスポンスやデジタルフォレンジックを行い、ボトムアップからの支援も担当。 2019 年 株式会社ラックに入社。 SDGs 達成に必要となる社会環境を予測し、 産業システム全般に必要となるセキュリティソリューションの企画開発を行う。
参加費	ＪＵＡＳ会員/ITC：67,400円 一般：85,800円（１名様あたり　消費税込み、テキスト込み）【受講権利枚数2枚】
会場	オンライン配信（指定会場はありません）
対象	情報システムの企画、開発、運用に従事している、あるいは従事予定の方。 「セキュリティ入門」の受講もしくは同等の知識を有していること。 初級
開催形式	講義・個人演習
定員	15名
取得ポイント	※ITC実践力ポイント対象のセミナーです。（2時間1ポイント）
特記	※当講座は、新型コロナウイルス感染症防止のため、オンライン受講のみとなります。
ITCA認定時間	12

主な内容

※当講座は、新型コロナウイルス感染症防止のため、オンライン受講のみとなります。
オンライン参加時のご注意について、本ページ下部にご案内いたします。お申込の前に必ずご確認ください。

～もう知らないでは許されない！セキュリティ技術を基礎から学ぼう～

企業の情報資産を保有・管理しているIT部門は、情報セキュリティの脅威と対策を理解する必要があります。情報セキュリティの脅威と対策を本質的に理解するためには、その基礎となる技術要素を理解する必要があります。

本講座では、IT担当者が直面する情報セキュリティ対策に関する基本的概念から、情報を保有する脅威と求められる対策（人的・技術的・物理的）における技術的な基礎知識を習得します。

*・:.。受講者の声.☆☆ ☆☆.。
・セキュリティに関することが体系的に理解でき、今までの断片的な知識が整理できた。
・情報量が多いが、後で見返しやすく復習しやすいテキストだった。
・講師の説明が丁寧で分かり易かった。詳細な内容についても簡潔に説明いただき、知識の習得に役立った。

・今後セキュリティについて学ぶための足掛かりになる。基礎講座として最適と感じた。
・全体が網羅されていて、また実体験も交えての講義で勉強になった。2日間やってくれるセキュリティ講座は珍しく、
内容が濃く良かった。人に薦めたい。
（20191128更新）☒
*・:.。.☆☆ ☆☆.。

第1章 セキュリティ基礎
１．情報セキュリティ
２．情報資産を守る
３．情報セキュリティマネジメントシステム
４．リスクアセスメント

第2章 コンプライアンスと運用セキュリティ
１．情報セキュリティ対策
２．情報セキュリティの運用
３．セキュリティ要素技術

第3章 脅威と脆弱性
１．攻撃の種類と特徴
２．アプリケーション攻撃の種類と特徴
３．無線攻撃の種類と特徴
４．ソーシャル・エンジニアリング攻撃の種類と特徴

第4章 ネットワークセキュリティ
１．ネットワーク機器と技術におけるセキュリティの機能と目的
２．ネットワークサービスとポート番号
３．セキュリティに関わるプロトコル

第5章 アプリケーション、データ、ホスティングセキュリティ
１．マルウェアの種類と特徴
２．ホストセキュリティの確立

第6章 アクセスコントロール、認証マネジメント
１．認証サービスの目的と機能
２．認証、認可、アクセスコントロール
３．アカウント管理を行う際のセキュリティコントロール

第7章 暗号化
１．暗号化
２．暗号アルゴリズム
３．暗号の種類

＜＜オンライン参加時のご注意＞＞
・紙媒体のテキストを開催おおよそ７日前に発送いたします。お申込み時に送付先の記入をお願いします。
・開催７日前から開催前日までにお申込の場合、テキスト送付がセミナー開催後になることがあります。ご了承ください。
・ご受講に必要なPC等のハードウェアや通信環境は、ご受講者様ご自身でご用意ください。
・動画や画像、音声の撮影、録画、録音は一切禁止とさせていただいております。
・キャンセル規定は「JUASセミナーキャンセル規定」と同様になります。

＜＜ライブセミナーご受講に際してのご注意＞＞
・ツールは、ZOOM（https://zoom.us/）を利用いたします。
・ZOOMミーティングID・PWは、開催日前に受講票にてご案内いたします。
・ブラウザまたは、ZOOMをダウンロード（無料）したPCをご利用ください。
ZOOMの紹介＞＞＞https://zoom.us/
ZOOMダウンロード＞＞＞https://zoom.us/signup

・ご参加いただくブラウザによって、制限がある場合がありますのでご注意ください。
・推奨ブラウザ：Google Chrome
（Internet Explorerのブラウザ版では、一部機能の制限があり、受講が難しい可能性があります。）
https://support.zoom.us/hc/ja/articles/214629443
初めてZOOMをご利用になる場合は、事前に接続テストを実施してください。
下記をクリックするとZoomの接続テストページにジャンプします。
https://zoom.us/test
・ユーザー名は、「お名前（漢字フルネーム）」に設定してください。
・セミナー当日は、15分前から受付開始いたします。待機室に入ってお待ちください。
事務局にて、お名前を確認させていただきます。
・ご参加の方には自己紹介（顔出しを含む）をお願いしております。皆様が不安を感じない
環境で開催をするための対応となりますのでご協力ください。