

## セキュリティ技術基礎【録画視聴】2024-02-28～03-13開催（4123261）

\*こちらは【2/14-15開催講座の録画視聴】となります\* 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	2024年2月28日(水) 録画配信開始 2024年2月29日(木) 2024年3月1日(金) 2024年3月2日(土) 2024年3月3日(日) 2024年3月4日(月) 2024年3月5日(火) 2024年3月6日(水) 2024年3月7日(木) 2024年3月8日(金) 2024年3月9日(土) 2024年3月10日(日) 2024年3月11日(月) 2024年3月12日(火) 2024年3月13日(水) 録画配信終了
カテゴリ	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 <a href="#">専門スキル</a>
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に従事する傍ら、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者として、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、人材育成などを担当。 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な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。 <a href="#">初級</a>
開催形式	録画視聴
定員	25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	*こちらは【2/14-15開催講座の録画視聴】となります *キャンセル規定について、録画開始日を開催日といたします。
ITCA認定時間	12

### 主な内容

#### ■受講形態

【選べる受講形態】

A. 会場orオンラインライブにてご参加：[お申込みは>>>こちら](#)

B. 録画視聴にてご受講：[【録画視聴のご注意】](#)

**※本ページは【録画視聴にてご受講】のお申込です。会場orオンラインライブにて参加希望の方は上記Aよりお申込みください。**

#### ■テキスト

配信開始7日前を目途に発送（お申込時に送付先の入力をお願いします）

※配信開始7日前から配信開始前日までにお申込の場合、テキストの送付が遅れる場合があります。ご了承ください。

■配信日までの課題事項

特になし

\*こちらは【2/14-15開催講座の録画視聴】となります\*

～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。内容が濃く良かった。人に薦めたい。

\*・:。☆☆☆☆。

## 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

-----  
<キャンセル規定>

録画配信日を開催日といたします。あらかじめご了承ください。

- ・土日祝を含む開催7日前から前々日まで…参加費用の50%
- ・土日祝を含む開催日前日および開催当日（欠席）…参加費の全額

※受講権利チケット利用にてお申し込みの場合

- ・土日祝を含む開催7日前から開催当日…参加費の全額（必要枚数）

※動画視聴前であってもキャンセル料が発生しますので、ご注意ください。