新人・配転者の方にオススメ！情報システムセキュリティ入門～システムで守る情報資産～（4119160）

新人・配転者の方にオススメ！情報システムセキュリティ入門～システムで守る情報資産～ ユーザー企業は、本当に自分の組織が必要としている情報システムセキュリティ要件を定義する能力が必要です。本セミナーでは、ユーザー企業が直面する情報システムセキュリティに関する課題への取り組み方や、情報を保有する本質的脅威と求められる対策を理解することを目的としています。

開催日時	2019年6月25日(火) 10:00-17:00
カテゴリー	IS戦略策定・IS戦略評価・IS企画・IS企画評価　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：33,000円 一般：42,000円（１名様あたり　消費税込み、テキスト込み）【受講権利枚数1枚】
会場	一般社団法人日本情報システム・ユーザー協会（日本橋堀留町2丁目ビル2階）
対象	情報システム部門若手・配転者の方、システム企画担当 初級
開催形式	講義、グループ演習
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	**＜事前アンケートご協力のお願い＞** セミナーの運営をより充実化するためお申込み時アンケートにご協力をお願いいたします。お申し込み後でもマイページより記入することができます。
ITCA認定時間	6

主な内容

○●受講者の声○●
・難しい用語なく、セキュリティ対策で大切なことを理解できた。
・事例から対策方法・考え方を学ぶことができた。
・自社の事例についても考えながら作業できたのが良かった。
・情報セキュリティに関してワークショップを通じて多角的に考えることができた。
・「情報セキュリティ」というと、難しくて面倒そうなイメージがあったが、わかりやすく
　どんな考え方を持てばよいか説明をしていただき、腹落ちできた。
・ワークショップを交えたグループ学習でいろいろな意見を聞けました。
・ユーザー企業がシステム構築をする際に見落としがちな点を教えていただいた。

==========
　本当に必要な情報システムセキュリティ要件を定義する能力を身につけよう！
==========

情報通信技術の普及と発展に伴い、組織の業務活動を効率化するために、
様々な業務処理が情報システム化されるようになりました。

しかし、情報システムを導入することで、業務システムが効率化される反面、
情報システム特有の課題である情報セキュリティの問題が発生するため、
情報セキュリティ対策に取り組んでいく必要があります。

情報セキュリティの問題は組織特有の問題のため、ベンダー任せの曖昧な情報セキュリティ要件ではなく、
本当に自分の組織が必要としている情報システムセキュリティ要件を定義する能力が、ユーザー企業側に求められます。

∴‥∵‥∴‥∵‥∴‥∴‥∵‥∴‥∵‥∴

本セミナーでは、知識学習と演習を取り扱うことで、ユーザー企業が直面する
情報システムセキュリティに関する課題への取り組み方や、
情報を保有する本質的脅威と求められる対策を理解することができます。
演習内容は、課題が存在するユーザー企業の情報システムを題材とすることでより実践的に学ぶことができます。

∴‥∵‥∴‥∵‥∴‥∴‥∵‥∴‥∵‥∴

<<内容>>　※変更する場合がございます。

1. 最近の情報セキュリティ事故事例

2. 情報システムの導入

3. 情報システム導入後の懸案事項
   情報システムの障害発生件数の推移
   障害事例
   システム障害の原因となりやすいポイント
   システム障害の影響

4. 情報システム利用時のトラブル
   情報システムが利用できない原因を考える
   ケース１　推察可能な問題
   ケース２　推察可能な問題
   情報システムが利用できない原因

5. 情報セキュリティ事故の事例
   情報セキュリティに関するキーワード
   情報セキュリティ事故の発生例
   ぜい弱性とは
   不正プログラムとは
   身近な情報セキュリティ事故を考えてみる
   情報セキュリティ事故事例と対策の例

6. 情報セキュリティ事故の特徴
   情報セキュリティ事故が発生する要因
   情報セキュリティ事故の特性
   情報システムセキュリティの共通的な特徴
   情報システムセキュリティの原則
   情報システムと情報セキュリティの関係
   情報システムで実装する情報セキュリティ対策（例）
   セキュリティが実装された情報システムの構築例

7. 情報システムセキュリティの原則
   情報セキュリティとは
   情報セキュリティ事故（機密性：情報漏えい）

法律の施行による情報セキュリティの普及
情報セキュリティ事故（完全性：情報改ざん）
情報セキュリティ事故（可用性：サービス停止）
情報セキュリティの対象範囲と保護要件の選択

8. 情報資産とは
情報システムセキュリティの対象範囲
情報資産を守るには
脅威、ぜい弱性

9. 情報システム設計時に要求されるリスクマネジメント
リスクと対策
情報セキュリティ事故が発生しやすい個所とは
情報セキュリティ事故の発生個所を想定する

10. 組織活動で期待される情報ライフサイクル管理
情報ライフサイクル
データライフサイクル
データに対する情報セキュリティ要件

11. 情報システムセキュリティの実装におけるユーザー企業の役割と責任
情報セキュリティマネジメント

12. 情報システムセキュリティの問題点を考える（ワークショップ）
演習

13.ブリーフィング（セミナーの振り返り）