はじめようCSIRT（シーサート）対応講座（4119280）

はじめようCSIRT（シーサート）対応講座
－ネットワークの盗聴・改ざん・漏洩・なりすまし対策講座－

ネットワークの盗聴・漏洩・なりすまし防止技術についての実務セミナーです。
本セミナーは下記の特徴を有しております。
・IPA(情報処理推進機構)のセキュリティガイドラインを考慮（対応）しております。
・CSIRT（Computer Security Incident Response Team、シーサート）に必要な機能や役立つ情報源の提示を行います。
・制御系、工場ネットワーク（イーサネット）での留意点を紹介します。
・IoT時代に対応したセキュリティに関する脆弱性と脅威について説明します。
・盗聴・改ざん・漏洩・なりすましなどの脅威について、事例と防御策・対応策について紹介します。

開催日時	2019年7月9日(火) 10:00-17:00
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
講師	上山勝也 氏 （株式会社上山システムラボラトリー　代表取締役 ） 民間企業のユーザー部門を経験後、豊田工業大学工学部制御情報工学科を首席で卒業。民間企業の情報システム部、(株)オープンシステム研究所、伊藤忠テクノサイエンス(株)を経て独立。現在は(株)上山システムラボラトリー代表取締役として、LANやイントラネットシステムの設計・運用・教育などのコンサルティング活動を展開。「無駄な出費をしないために、今あるシステムを有効に使っていく、システムの更新をするにしても将来にわたって無駄のない設計や改善を行う。そしてそれを支える要員の育成をしていく。お客様といっしょにシステムを適切に発展させる。」のが基本的なスタンス。 ＜主な資格＞オンライン情報処理技術者、ネットワークスペシャリスト、システム監査技術者
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	◆対象：　・情報系及び工場系のセキュリティ対応を把握したい方 ・これからCSIRTの構築、活動をしたい方　・CSIRTでの活動に役立てたい方 ・脆弱性情報を含めたセキュリティ関連情報の入手の仕方や見方を知りたい方 ・各種ガイドラインにそったセキュリティ対応活動をされたい方 ・盗聴・改ざん・漏洩・なりすましなどへの対応をされたい方　◆受講前提条件： ・ネットワークについて基本的な技術・用語についての知識をお持ちの方 ・サイバーセキュリティについて基本的な技術・用語についての知識をお持ちの方 中級
開催形式	講義
定員	30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	◆受講特典：（希望者に電子データ【メール配信】でご提供） 【民間企業の方】 ・IPAから提供されている「サイバーセキュリティ経営ガイドライン」をベースにした「サイバーセキュリティ対策チェックリスト」 【政府系の方】 ・IPAから提供されている「地方公共団体における情報セキュリティ対策基準平成３０年」の要約版 【必要な方】 ・サイバーセキュリティに関する報道事例集 ・サイバーセキュリティに関する被害事例集 ・情報セキュリティ対象マトリックスIoT版（エクセルですので加工頂けます）
ITCA認定番号	ITCC-CPJU9436
ITCA認定時間	6

主な内容

本企画は、ネットワークの盗聴・漏洩・なりすまし防止技術についての実務セミナーです。

サイバーセキュリティの脅威はますます増大しており、2020年オリンピックに向けて、国際的なサイバーテロ意識した、官民合わせての対応が求められてきています。具体的には、IPAやJPSERT各種情報系独立行政法人、セキュリティセンターなどは各種ガイドラインや脆弱性レポートを提供するなど、啓蒙やインシデント対応、対応策の助けになる活動を行っています。しかしながら、サイバー攻撃の主体が標的型攻撃に移行してきており、これまでは比較的安全とされてきた、工場系の制御システムを含めたネットワークへのサイバー攻撃が以前よりも増してきています。IoTの進展にともって、これまで安全とされてきた領域での脆弱化が懸念され、まずます、盗聴・改ざん・漏洩・なりすましなどの脅威への対応が必要になってきています。

本セミナーは下記の特徴を有しております。
・IPA(情報処理推進機構)のセキュリティガイドラインを考慮（対応）しております。
・CSIRT（Computer Security Incident Response Team、シーサート）に必要な機能や役立つ情報源の提示を行います。
・制御系、工場ネットワーク（イーサネット）での留意点を紹介します。
・IoT時代に対応したセキュリティに関する脆弱性と脅威について説明します。
・盗聴・改ざん・漏洩・なりすましなどの脅威について、事例と防御策・対応策について紹介します。

＜内容＞
第１部　CSIRT（シーサート）とは
１　インシデントの対応と CSIRT
２　CSIRT 構築について（組織構築、チーム構築、役割などスタートアップに必要な要素を解説します）
３　情報収集と現状把握・問題把握（効率的、機能的な活動を行なうために必要なアクションプランを説明します）
４　想定される要員のスキルや技術力、アサイン、育成方法について

第２部　CSIRT活動を支援する機関・ツールの紹介
１　JPCERT/CCについて
２　JVNとCVSSについて（脆弱性情報の入手方法・見方・その後のアクションプランを説明します）
３　IPAについて
４　情報セキュリティ関連ガイドラインについて（各種ガイドラインの位置づけと基本的な内容を説明します）

第３部　制御系、工場ネットワーク（イーサネット）での留意点
１　鎖国されていたはずのネットワークに黒船がやってきた！
２　導入当初安全だったが、現在はかならずしもそうではない！
３　なぜ侵入されるのか？
４　制御系、工場ネットワークで考慮すべき技術要素について

第４部　IoT導入におけるセキュリティ設計のポイント
１　IoTに関するセキュリティ脅威について（なぜIoTが狙われるのか）
２　IoTセキュリティ問題の事例
３　IoTのセキュリティ設計のポイント
４　開発段階でのポイント
５　運用・保守段階でのポイント
６　IPAなど各種コンテンツの活用について

第５部　標的型攻撃（盗聴・改ざん・漏洩・なりすまし）への対応
１　執拗な標的型攻撃について
２　オーソドックスな攻撃シナリオ（計画・準備・潜入【初期・構築・調査】・実行）
３　マルウェア感染
４　バックドア開設
５　諜報活動・調査探索
６　侵害活動・サーバへの拡大
７　データ窃取・データ破壊・業務妨害
８　対策手法の紹介