ネットワークセキュリティ技術基礎講座（4119267）

ネットワークセキュリティ技術基礎講座
－ネットワークの盗聴・改ざん・漏洩・なりすまし等への対応

ネットワーク管理に必要なセキュリティ技術の基礎講座です。
本セミナーはネットワークセキュリティの対象となるデバイス類と導入時における留意点、ネットワークに対する主な脅威と対応ポイントの解説、無意識のうちに使われることもあるIPv6の問題点（注意する点）について指摘します。制御系、工場ネットワーク（イーサネット）での留意点や今後拡大が予想されるIoT導入におけるセキュリティ設計のポイントについてその要点を説明します。

開催日時	2019年8月20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（ユニゾ堀留町二丁目ビル2階）
対象	◆対象：発注者としてネットワークの基本設計・RFP作成を担当される方、ネットワークの調達担当者 ◆受講者のレベル：　・LAN・WANの基礎知識がある方 ・LAN・WANの運用管理等の業務に取り組まれ、さらにスキルアップを目指す方 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）
ITCA認定番号	ITCC-CPJU9432
ITCA認定時間	6

主な内容

ネットワーク管理に必要なセキュリティ技術の基礎講座です。

本セミナーはネットワークセキュリティの対象となるデバイス類と導入時における留意点、ネットワークに対する主な脅威と対応ポイントの解説、無意識のうちに使われることもあるIPv6の問題点（注意する点）について指摘します。制御系、工場ネットワーク（イーサネット）での留意点や今後拡大が予想されるIoT導入におけるセキュリティ設計のポイントについてその要点を説明します。

ネットワークセキュリティそのものを学ばれたい方はもちろん、ネットワークインフラ構築、日常のネットワーク運用においてもセキュリティを考慮することは重要になっていますので、ネット
ワークセキュリティに関する構築や運用・保守業務に直接関係しない方にも有用な内容です。

ユーザー企業でセキュリティ構築を経験し、現在はネットワークシステム構築のプロジェクトマネージャー、コンサルタント、SIerセキュリティ要員として従事し、JUASにおいて各方面での講演をしている講師が講義を担当します。

＜内容＞

第１部　はじめに

第２部　ネットワーク機密管理の対象となるデバイス類と導入時における留意点
　　－対象となるデバイス類と防御機構についてのRFP作成上の留意点を解説します。
　１．クライアント、サーバー（アプリケーション／DB、メール、ゲートウェイ、DNS、DHCP、プロキシなど）
　２．各種スイッチ
　３．無線LANデバイス（無線LAN－AP）
　４．フィルタリング（ACL）、ファイヤーウォール
　５．WAF（Web Application Firewall）
　６．IDS／IPS（不正侵入検知／防止システム）

第３部　ネットワークに対する主な脅威と対応ポイントの解説
　　－基本的な用語の説明だけでなく、どのよう点に留意してRFPに盛り込むかのポイントを解説します。
　１．コマンドインジェクション
　２．SQLインジェクション
　３．ディレクトリトラバーサル（パストラバーサル）
　４．バッファオーバーラン（バッファオーバーフロー）
　５．DoS、DDoSアタック
　６．セッションハイジャック
　７．クロスサイトリクエストフォージェリ（CSRF）
　８．クロスサイトスクリプティング（XSS）
　９．フィッシング
１０．バグとセキュリティホール
１１．ウイルス・ワーム・スパイウェア・ランサムウェア
１２．SPAM
１３.今後も拡大する対象（漏洩・なりすまし・改ざん・スローダウンなどの視点でクリア）
１４．今後、どのよう点に留意して機密に対応していくかのポイント

第４部　IPｖ６のダークサイド（暗黒面：注意しないとはまります）
　　－無意識のうちに使われることもあるIPｖ６についての問題点を指摘します。
　１．IPv6とは（簡単に前提ご説明）
　２．ネットワーク（機器）負荷増大
　３．自動化技術が運用に穴をあける
　４．安易な設定がセキュリティ強度を弱くする（脆弱性を生む）

第５部　制御系、工場ネットワーク（イーサネット）での留意点
　　－安全であるはずだった工場ネットワークについての考慮すべき技術要素を解説します。
　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！（工場NETについても簡単に前提ご説明）
　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６部　IoT導入におけるセキュリティ設計のポイント
　　－IoT導入におけるセキュリティ対応のポイントを解説します。
　１．IoTとは（簡単に前提ご説明）
　２．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）
　３．IoTセキュリティ問題の事例
　４．IoTのセキュリティ設計のポイント