ネットワーク監視とログ解析の勘所～集め方、分析技法、危機予兆・知見の獲得方法【オンラインライブ】（4123204）

本セミナーでは、各種ログのポイント、パケット状況のパターン解説、効率的な解析手法など、ネットワーク診断、トラブルチェック、セキュリティチェックに特化した解説を行います。ユーザー企業・ベンダーにおいてネットワーク診断に従事し、トラブルシューティング系の出版を行い、現在はネットワーク設計やネットワーク診断レポート作成・トラブルシューティング業務に従事している講師が講義を担当致します。

開催日時	2023年7月20日(木) 9:00-16:00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	What(DXで活用されるデータ・技術)：デジタル技術　How(データ・技術の活用)：留意点
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：33,800円 一般：43,000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	オンライン配信（指定会場はありません）
対象	・ネットワークの運用管理に取り組まれ、さらにスキルアップを目指す方 ・パケットキャプチャと分析を始めたい方 ・ログの効率的な解析を行いたい方 ◆受講者のレベル： ・ネットワークの基礎知識がある方 中級
開催形式	講義
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）
ITCA認定時間	6

主な内容

■受講形態
ライブ配信（Zoomミーティング）【セミナーのオンライン受講について 】
■テキスト
開催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）
■開催日までの課題事項
特になし

本セミナーでは、各種ログのポイント、パケット状況のパターン解説、効率的な解析手法など、ネットワーク診断、トラブルチェック、セキュリティチェックに特化した解説を行います。
ユーザー企業・ベンダーにおいてネットワーク診断に従事し、トラブルシューティング系の出版を行い、現在はネットワーク設計やネットワーク診断レポート作成・トラブルシューティング業務に従事している講師が講義を担当致します。

（講師の言葉）
理論も必要ですが、実践こそが重要です。
近年IoT化の進展に伴い、ネットワーク関連のハードウェアやソフトウェアが充実し、ユーザー数も増え、管理対象の種類と量が増大してきています。
それに伴いネットワークが停止・スローダウンしたときの影響は以前にも増して重大なものとなっていることは、ご存知のとおりです。特

に最近では「快適に使用できる」というSLA要件を満足させることが重要であり、スローダウン対策やトラブルの早期解決について、ネットワーク管理者への要求が高まってきています。
加えて、執拗なサイバー攻撃の増大により、防御システムによる「大丈夫なはず」というスタンスでは、防除できず、各種ログのインシデント発生時の適切な活用と平時における活用が重要になってきています。
このような中、ネットワーク正常化、安定化稼働への有効なアクションとして技術者のスキルアップとツールの導入が以前にも増して求められてきています。

■主な内容
第1部 ネットワーク管理の基本
ネットワーク管理の全体像について解説します。
１．ネットワーク管理の重要性
２．ネットワーク管理エネルギー増大の法則について
３．ネットワーク管理の全体像
４．障害管理・性能管理と構成管理・機密管理・課金管理
５．代表的な管理ツールの紹介（役割の違いも説明）
６．SNMP、パケットキャプチャ、ログについて

第2部 ログによる解析と監視
１．ログ管理とその目的
２．ログの種類
３．ログファイル管理（集約化についても）
４．ログ解析（デジタルフォレンジックについても）
５．SIEMについて

第3部 監視技術と防御技術
１．監視技術について
２．スキャン方式について（ウイルススキャン、アクセススキャン、メールスキャンについても）
３．防御技術について
４．フィルタリングについて
５．コンテンツフィルタリングについて

第4部 ネットワーク防御構成と、ログポイント（集めるツール、集める場所）
１．セグメント分割・DMZについて
２．インターネット接続の防御ポイント
３．各種サーバ（Web、メール、DNS）分割化の必要性
４．リバースプロキシのログ活用ポイント

第5部 侵入検知・防止システム（監視体制とそのポイント）
１．IDSについて（種類と配置）
２．IPSについて（種類と配置）
３．フォールスポジティブとフォールスネガティブ
４．IDS/IPSログ活用留意点

第6部 効果的なログ解析（ログ整理、分析方法と危機予兆のつかみ方）
１．事前設定の重要性（準備が適切でないと、いざという時に役に立たないログ収集になっている）
２．ソーティングの活用
３．フィルタリング、検索の活用
４．定期的なログチェックの重要性
５．IPA試験から、ログ関連問題を取り上げた演習