21j　ログ監視環境の構築とログ解析実践
（New）

1. 研修要領

・募集定員　16名
・研修会場　出島交流会館

・講　師　富士通九州システムズ（FJQS） 太田伸一郎
・開催月日　2020年01月15日（水）・16日(木)・17日（金）
・実施時間・日数　9:30 ～ 17:30 （7時間/日）・3日間（21時間）
・受 講 料（税別）　78,800円
・教 材 料（税別）　5,000円

2. 対象者

セキュリティインシデント対応を行う方
前提としてセキュリティの基礎知識、Linux/WindowsServerの操作経験が必要です

3. カリキュラムの概要

本コースでは、Windows/LinuxなどOS、WebサーバやDNSサーバ、Proxyサーバー、Mailサーバー、FTPサービス、ファイル共有サーバ、ルーター、データベースなどの**各種ログの形式を学習し、セキュリティに関するインシデント対応で必要となるログ解析スキルを習得**します。

先ず、各システムで必要な**ログ環境の構築**（環境設定）を行います。

ログのフォーマットや採取したログの見方を理解いただいたうえで、実際にインシデント対応時に必要となるログファイルの分析方法について**実機を使用して確認**します。

4. カリキュラムの詳細　3日間（21時間）

科目	時間	科目の内容
1. ログ概論	2.0hr	・ログとは、ログの目的 ・ログの記録方法、ログの保存期間 ・ログファイルの分割 ・ログの運用 ・ログの設定、ログの分析
2. Windowsのログ	2.0hr	・Windowsのログ ・イベントログの構造 ・EVT形式のイベントログ、EVTX形式のイベントログ ・イベントログのアーカイブ ・複数PCのイベントログ参照 ・監査、監査ポリシー　【実機演習】
3. Linuxのログ	2.0hr	・Linuxのログ ・ログファイルのチェック、アクセスログの調査 ・rsyslog、rsyslogの設定 ・セッションログ(SSH)、セッションログ(Telnet) ・認証ログ　【実機演習】
4. DNSサーバのログ	2.0hr	・DNSサーバのログ ・BIND独自のログ ・カテゴリの種類 ・クエリーの記録 ・クエリーログのON/OFF　【実機演習】
5. Webサーバのログ	2.0hr	・Webサーバ(apache)のログ ・エラーログ、アクセスログ ・ステータスコード ・ログフォーマット ・リクエスト内容 ・Apacheログの解析ツール

科目	時間	科目の内容
6. FTPサーバのログ	1.0hr	・FTPサーバ(vsftpd)のログ ・ログモードの変更 【実機演習】
7. Mailサーバのログ	1.0hr	・SMTPログ ・ログの項目 ・PostFixログ解析ツール 【実機演習】
8. ファイル共有サーバのログ	1.0hr	・ファイル共有(Samba) ・Sambaのログ ・ログオプション ・ファイル共有(Samba)の監査 【実機演習】
9. IISのログ	2.0hr	・IISのログ ・Webサイトのログ設定 ・FTPサイトのログ設定 【実機演習】
10. Proxyサーバのログ	2.0hr	・Proxyサーバのログ ・storeログ、accessログ ・ログ解析ツール 【実機演習】
11. データベースのログ	1.0hr	・データベースの監査ログ ・Oracle Databaseの監査 ・SQL Serverの監査 ・PostgreSQLの監査
12. ルータのログ	1.0hr	・Ciscoルータの基礎 ・ルータログのsyslog転送
13. ログ解析ツール	2.0hr	・ログ解析ツール ・LogParser ・Event Log Explorer ・iLogScanner ・EventLog Analyze 【実機演習】
計	21.0hr	

5. 使用教材
ログ監視環境の構築とログ解析実践(FJQS教材)
FJQSオリジナル問題集

6. 到達目標

本コース修了後、次の事項ができることを目標としています。
1. Windows/Linuxのログ環境を作成できる。
2. ログの種類や記述内容を理解できる。
3. Windows/Linuxの各種ログ内容を理解できる。
4. 主要なサーバーアプリケーションのログについて理解できる。
5. セキュリティに関するインシデント対応時に必要なログを判断できる

7. レベル
ITSS:ITスペシャリスト育成 - [*]テクノロジ【レベル:2-3】
ITSS:アプリケーションスペシャリスト育成 - [*]テクノロジ【レベル:2-3】

[*] ITスキル標準研修ロードマップにおけるコース群名