AIを活用したセキュリティ防御術バラマキ型ランサムウェア対策【会場】（4126258）

本セミナーは、ゼロトラストFTAの考え方とAIを使って作成したネットワークデジタルカルテを軸に、皆さんの会社のセキュリティを守ることを目的とした企画です。システム管理者が「何をしたいか」という目的意識を持ち、AIにコマンド出力やログを読み込ませながら高精度な分析を行う方法論を、講義とハンズオンで体験します。

開催日時	2026年12月3日(木) 10:00-17:00会場
JUAS研修分類	セキュリティ(サイバーセキュリティ)
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	吉田晋 氏 （株式会社コネクトワン　代表取締役 ） 中小企業から大企業まで幅広いIT支援を手がける。独自のセキュリティ診断フレームワーク「ゼロトラストFTA」を開発・実践し、AIを活用したネットワークデジタルカルテ作成の方法論を確立。現在「ゼロトラストFTA（AIと読むセキュリティ読本）」を執筆中。
参加費	JUAS会員企業/ITC：35,200円 一般：45,100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（NBF東銀座スクエア２F）
対象	・大企業の情報システム部門の管理者・担当者 ・ランサムウェア対策の見直しを検討している方 ・AIをセキュリティ業務に活用したい方 中級
開催形式	講義・個人演習
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	PC持参。AI利用環境（ChatGPT・Claude等）を事前にご準備ください。
ITCA認定時間	6

主な内容

■受講形態
会場のみ（オンラインなし）
■テキスト
当日配布
■開催日までの課題事項
PC持参。AI利用環境（ChatGPT・Claude等）を事前にご準備ください。

AIを活用したセキュリティ防御術バラマキ型ランサムウェア対策
― 架空の企業ネットワークをAIと分析し、侵入・拡散を封じる防御設計を体験する ―

本セミナーは、ゼロトラストFTAの考え方とAIを使って作成したネットワークデジタルカルテを軸に、皆さんの会社のセキュリティを守ることを目的とした企画です。
システム管理者が「何をしたいか」という目的意識を持ち、AIにコマンド出力やログを読み込ませながら高精度な分析を行う方法論を、講義とハンズオンで体験します。
今回は最も多い攻撃パターンであるバラマキ型ランサムウェアを取り上げます。
架空の大企業（精密機器メーカー、連結約8,500名、国内外複数拠点・工場）のネットワークデジタルカルテを教材として、AIと対話しながら「どこから侵入する確率が高いか」を分析し、多層防御の優先設計を体験します。

◆学習目標
・バラマキ型ランサムウェアの侵入手口と大企業内での拡散メカニズムを理解する
・ゼロトラストFTAを使ってアタックサーフェスとクラウンジュエルを可視化する方法を習得する
・AIと対話しながら侵入確率の高い経路を分析し、防御優先順位を導き出す手法を体験する

第１部 ゼロトラストFTAとAI活用の３原則
（1）AIとシステム管理の親和性 ―― 管理者が「何をしたいか」を持ち、AIが「どう設定・解析するか」を補完する
（2）AI活用の３原則：①目的意識（ゼロトラストFTAで守る範囲を定める） ②コマンドと管理画面（対話の入力基本） ③ネットワークデジタルカルテ（設定値・ログをAIが解析できる形に整理）
（3）架空企業のカルテ概要と本日のシナリオ説明
第２部 バラマキ型ランサムウェアの手口
（1）バラマキ型と粘着標的型の違い
（2）初期侵入から拡散までの典型経路（メール・脆弱性・VPN）
（3）大企業特有のリスク：OT連携・拠点間VPN・バックアップ
第３部 ハンズオン：AIと一緒に攻撃経路を分析・防御設計する
（1）架空企業のカルテをAIに読み込ませ、侵入・拡散経路を対話で追跡する
（2）防御の盲点と優先対策をAIと一緒に洗い出す
（3）多層防御の設計案を参加者がまとめる
第４部 まとめとディスカッション
（1）参加者による分析結果の共有
（2）自社に持ち帰る「明日からできること」の整理

◆前提条件：
PC持参。AI利用環境（ChatGPT・Claude等）を事前にご準備ください。