セキュリティリスク分析ツール

を使う３つの理由

弊社では、IPA(情報処理推進機構) が推進している
「制御システムのセキュリティリスク分析ガイド」
を強力にサポートするためのリスク分析ツールを
提供しています（無償 / 有償）。
ここで、そのツールを利用する３つの理由をご紹介します。

1. 工数が激減する

リスク分析において最も工数がかかるのは、分析する対象のシステムを IPA の推奨する手法にあてはめるためのフォーマットに落とし込む必要があります。

このフォーマットは、IPA から提供されているものの、分析対象に併せて分析されるお客様が独自に追加しなければなりません。手作業で何百もの攻撃ツリーを作成するための工数、間違いが無いかをチェックするための工数が実は膨大なのです。弊社リスク分析ツールではこのシートを数秒で作成可能です。

2. 攻撃ツリーの選択のための基準が一定になる

リスク分析において、多くの情報が必要なのは、「どの攻撃ツリーが危ないのか？」を判断する事です。IPA の分析手法では、資産の接続関係やデータフローの有無で危険度を判定しますが、定量的な判定方法は定まっていません。弊社ツリーでは、資産のルートの可能性ある組み合わせとデータフロー有無に関連する独自のパラメータで、危険なルートを、危険度という評価関数で数値化しています。分析者は、その数値から分析候補を簡単で同じ基準で選択する事ができます。

3. 手厚いサポート

IPA では、制御システムのセキュリティリスク分析ガイドのサポートとして、入門セミナーは不定期に開催していますが、実践編セミナーや実習プログラムも用意されていません。また、独法であり公平性の観点から、個別サポートは困難です。
弊社では各種のサポートをフレキシブルに行う事が可能です。

どうしても避けては通れないリスク分析を最も効率良く行う一つの選択肢として INJANET の提案をご検討ください。

rev.202010

INJANET 株式会社

info@injanet.co.jp
東京都立川市
錦町 6-23-10