制御システムのセキュリティリスク分析ガイド オンラインセミナー　2024年度下期　開催のご案内

制御システムに対するサイバー攻撃によって、大規模停電や燃料パイプラインの供給停止、製造業における生産停止や設備破壊など、事業に重大な影響を及ぼす事例も発生しています。このような中、制御システムの保有事業者において、運用・制御技術に対する脅威及び対策の必要性の認識が進んでいます。

IPAでは、セキュリティ確保のためのリスクマネジメント強化手法として近年注目されているリスクアセメントの3つのプロセス（リスク特定・リスク分析・リスク評価）の中でも、中心的な作業であるリスク分析にフォーカスして解説した『制御システムのセキュリティリスク分析ガイド』（以下、分析ガイド）を公開しています。

本セミナーでは、リスク分析の全体像と共に、分析ガイドで紹介している2種類のリスク分析手法（資産ベースのリスク分析、事業被害ベースのリスク分析）の具体的な実施手順を解説します。

講義動画の内容は、上期開催と同一です。制御システムにおけるリスク分析の重要性と『分析ガイド』の概要を解説する「概要編」（2023年度までの「管理者向け概説動画」を改題・改定）を公開しています。

主催	独立行政法人情報処理推進機構（IPA）
開催期間	2024年12月2日（月）10:00 ～ 2025年3月31日（月）17:00
開催方法	開催期間中、受講者に対して以下を提供いたします。 ① 講義動画（概要編 約35分※、入門編 約2時間40分、応用編 約1時間15分）をYouTubeで配信 ・開催期間中は、いつでも、ご自身のペースで、繰り返しご視聴できます。 ② 電子メールによる質疑応答 受講を希望される方は、YouTubeの動画視聴環境、IPAとのメール送受信環境が必要です。
定員	400名程度
受講費	**無料**
募集対象	①制御システムを保有する事業者の方 ②制御システムのインテグレーター、ベンダー、メーカーの方 ③制御システムのリスク分析に興味のある方 開催期間中に定員以上の受講希望があった場合は、1法人・団体あたりの受講者を制限させて頂くこと等がございます。予めご了承をお願いいたします。
セミナーで学べること	セキュリティ対策としてのリスク分析の有効性及びリスク分析についての理解を深め、具体的なリスク分析の実施方法と、投入可能な人員及び予算の範囲で出来るだけ効果的にリスク分析を行う方法を学ぶことができます。
テキスト	『制御システムのセキュリティリスク分析ガイド 第２版（2023年3月版）』（入門編） 『制御システムに対するリスク分析の実施例 第２版（2023年12月版）』（応用編） を使用します。テキストのPDFファイルは、IPAのウェブサイトより各自ダウンロードしてください。

※・・・「概要編」講義動画は、以下のURLにて、受講申込み前に視聴可能です。https://youtu.be/Ub8_aMxxpzU

お申込み方法

以下のWebサイトに掲載したお申込み方法に従い、セミナー事務局までお申し込みください。

https://www.ipa.go.jp/security/seminar/controlsystem/riskanalysis2024-2h.html

IPA 独立行政法人情報処理推進機構 セキュリティセンター

制御システムのセキュリティリスク分析ガイドセミナー事務局
E-mail : isec-ics-semi@ipa.go.jp

制御システムの
セキュリティリスク分析ガイド 第2版

「**リスク分析**」は、サイバー攻撃に対するリスクを低減する重要なプロセスです。本ガイドは、**リスク分析**を中心とした、制御システムの「**リスクアセスメント**」の具体的な手順を解説した実践的な手引きです。制御システムを保有する事業者自身で**リスクアセスメント**の実施が可能となります。

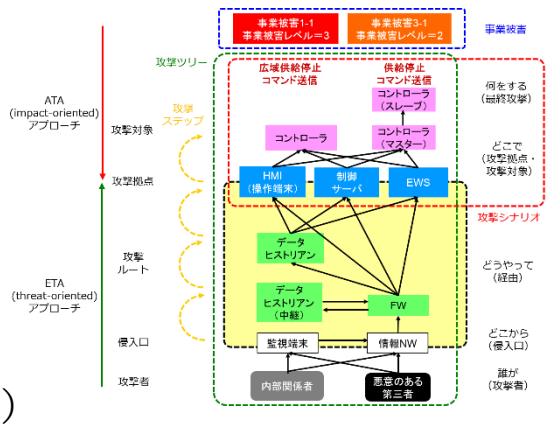
「**リスク分析**」＝ 制御システムやそれによって実現している事業の重要性、想定される脅威とその発生可能性、脅威に対するセキュリティ対策状況／脆弱性を評価し、相対評価可能な「リスク値」として把握するプロセス

「**リスクアセスメント**」＝ リスク特定、リスク分析及びリスク評価のプロセス全体

事業に多大な被害を及ぼすリスクの高い箇所やリスク低減に最も効果的な個所を特定し、優先順位付けしたセキュリティ投資が可能となります。時間経過に従い発生する新たな脅威に対して、リスクアセスメントのPDCAサイクルを確立し、継続的なリスク低減が可能となります。

ガイドの概要と特徴

- リスク分析の具体的な実施手順を提示
- 2通りの**詳細リスク分析の手法**を解説
  - **資産ベースのリスク分析**
  - **事業被害ベースのリスク分析**
- **リスク分析のための素材**の提供
  （リスク分析シートのフォーマットと実施例、他）
- リスク分析結果の**活用例**の提示
  （対策強化策の検討方法、セキュリティテストの解説）



【事業被害、攻撃シナリオ、攻撃ツリーの関係】

ガイド本編の目次

【ガイド本編】400頁

【別冊】102頁

【活用の手引き】
37頁

IPA 制御 リスク分析ガイド 検索

https://www.ipa.go.jp/security/controlsystem/riskanalysis.html

独立行政法人**情報処理推進機構**
セキュリティセンター

制御システムセキュリティ問合せ窓口
E-mail : isec-ics@ipa.go.jp