CSSCの制御システムセキュリティ教育

2020年12月

技術研究組合制御システムセキュリティセンター

CSSCの制御システムセキュリティ教育について

技術研究組合制御システムセキュリティセンター（CSSC）は、制御システムセキュリティの研究とともに、普及啓発活動を通して、制御システムセキュリティ教育に関する独自のコンテンツを開発して参りました。

そうした独自のコンテンツを活用し、制御システムセキュリティ教育に関してお悩みの方に教育機会をご提供する所存です。

CSSCの制御システムセキュリテイ教育の特徴は、次頁にございますように、幅広いニーズに対応するために座学と実習を組み合わせ、実習の際には模擬プラントを活用すること等です。

本資料をご参照頂き、CSSCの制御システムセキュリティサービス活用をご検討下さいますようお願い申し上げます。

技術研究組合制御システムセキュリティセンター
事務局長　村瀬一郎

CSSCの制御システムセキュリティ教育概要

特徴

1) 基礎、インシデントハンドリング、リスクアセスメント、ペネトレーションテスト、評価認証等幅広い分野の教育コース
2) 事業者、ベンダ等幅広い対象を想定したコース
3) 座学と実習を必要に応じて組み合わせ
4) 模擬プラント（または可搬型模擬プラント）を用いた実習
5) グループディスカッションを取り入れた参加型教育

教育コース

1) 制御システムセキュリティ基礎
2) インシデントハンドリング
3) リスクアセスメント
4) ペネトレーションテスト
5) 評価認証（詳細省略）

何れも日数、教育内容等は相談可能です。

制御システムセキュリティ基礎コース

１．目的
　制御機器や制御システムのセキュリティに関して今後業務にて関わりを有する方が知っておくべき基礎的事項を習得する。
２．対象
　制御システムセキュリティに興味をお持ちの方。
３．場所
　多賀城または御社ご指定の場所。
４．日時
　別途御相談。
５．費用等
　数十万円から。
６．人数
　多賀城の場合最大30人。
７．プログラム内容案

時間	内容
10分	オープニング
60分	制御システムセキュリティの脅威と対策の基礎
30分	模擬プラントまたは可搬型模擬プラントを用いた演習
50分	グループディスカッション（社外からの問い合わせ対応に際して知っておくべきこと）

インシデントハンドリングコース

１．目的
　制御システムの異常の原因峻別、および制御システムにおけるサイバーセキュリティインシデント対応の知見を蓄積する。
２．対象
　制御システムの運用に従事されている方。
３．場所
　多賀城または御社ご指定の場所。
４．日時
　別途御相談。
５．費用等
　ご相談。
６．人数
　多賀城の場合最大30人。

インシデントハンドリングコース

7．プログラム内容案

開始時刻	時間	内容
9:30	10分	オープニング
9:40	60分	制御システムセキュリティの脅威と対策の基礎
10:50	70分	定圧制御模擬プラントを用いた演習（模擬攻撃演習）
12:00	60分	昼食
13:00	70分	水位一定制御模擬プラントを用いた演習（トレンドグラフ解析による原因峻別）
14:20	80分	制御システムにおける緊急時の対策
15:50	80分	制御システムにおける証跡の追跡
17:20	20分	まとめ

リスクアセスメントコース

1．目的
　制御機器や制御システムのベンダの技術者が、制御システムセキュリティ技術の脅威と対策の概要とリスクアセスメントの手法を習得する。
2．対象
　制御機器や制御システムに従事する技術者。制御システムセキュリティ対策を推進する立場にある方が望ましい。
3．場所
　御社ご指定の場所。
4．日時
　別途御相談。
5．費用等
　ご相談。
6．人数
　最大50人程度。
7．プログラム内容案

時間	内容
10分	オープニング
40分	制御システムセキュリティの対策の詳細
30分	可搬型模擬プラントを用いた演習
40分	リスクアセスメント手法の概要（リスクアセスメント手法の概要、典型的なサイバー攻撃シナリオ）
60分	リスクアセスメント演習（典型的な制御システムを想定した演習）

リスクアセスメントコース

1．目的
　制御機器や制御システムのベンダの技術者が、制御システムセキュリティ技術の脅威と対策の概要とリスクアセスメントの手法を習得する。
2．対象
　制御機器や制御システムに従事する技術者。制御システムセキュリティ対策を推進する立場にある方が望ましい。
3．場所
　御社ご指定の場所。
4．日時
　別途御相談。
5．費用等
　ご相談。
6．人数
　最大50人程度。
7．プログラム内容案

時間	内容
10分	オープニング
40分	制御システムセキュリティの対策の詳細
30分	可搬型模擬プラントを用いた演習
40分	リスクアセスメント手法の概要（リスクアセスメント手法の概要、典型的なサイバー攻撃シナリオ）
60分	リスクアセスメント演習（典型的な制御システムを想定した演習）

ペネトレーションテストコース(1)

1．目的
　制御機器や制御システムのベンダの技術者が、制御システムセキュリティ技術の脅威と対策の概要とペネトレーションテストの手法を習得する。
2．対象
　制御機器や制御システムに従事する技術者であり、セキュリティ検証の担当者。
3．場所
御社ご指定の場所。
4．日時
　別途御相談。
5．費用等
　数百万円
6．人数
　1回あたり最大30人程度。

ペネトレーションテストコース(2)

7. プログラム内容案
（1）多賀城の場合

1日目			
9:30	9:40	10	オープニング
9:40	10:45	65	制御システムセキュリティの脅威と対策の基礎
10:55	12:00	65	制御システムにおける対策の詳細
昼食			
13:00	14:05	65	火力発電訓練シミュレータを用いた演習
14:05	14:30	25	監視カメラを用いた演習
14:45	16:00	75	変電所監視制御システムを用いた演習
16:15	17:30	75	制御システムセキュリティにおけるヒューマンファクター
2日目			
9:15	10:30	75	定圧制御模擬プラントを用いた演習
10:45	12:00	75	水位一定制御模擬プラントを用いた演習
昼食			
13:00	14:05	65	セキュリティ検証の概要
14:15	16:00	105	ペネトレーションテストの概要
16:15	17:30	75	ペネトレーションテストの活用方法
3日目			
9:15	10:30	75	ペネトレーションテスト実習(1)
10:45	12:00	75	ペネトレーションテスト実習(2)
昼食			
13:00	14:15	75	ペネトレーションテスト実習(3)
14:30	15:45	75	ペネトレーションテスト実習(4)
16:00	17:15	75	ペネトレーションテスト実習(5)
17:15	17:30	10	クロージング

ペネトレーションテストコース(3)

7. プログラム内容案
(2)出張型の場合

1日目			
9:30	9:40	10	オープニング
9:40	10:45	65	制御システムセキュリティの脅威と対策の基礎
10:55	12:00	65	制御システムセキュリティの対策の詳細
昼食			
13:00	14:05	65	セキュリティ検証の概要
14:15	16:00	105	ペネトレーションテストの概要
16:15	17:30	75	ペネトレーションテストの活用方法
2日目			
9:15	10:30	75	ペネトレーションテスト実習(1)
10:45	12:00	75	ペネトレーションテスト実習(2)
昼食			
13:00	14:15	75	ペネトレーションテスト実習(3)
14:30	15:45	75	ペネトレーションテスト実習(4)
16:00	17:15	75	ペネトレーションテスト実習(5)
17:15	17:30	10	クロージング