

技術研究組合制御システムセキュリティセンター (CSSC) のご紹介

2026年3月12日

技術研究組合制御システムセキュリティセンター (CSSC)

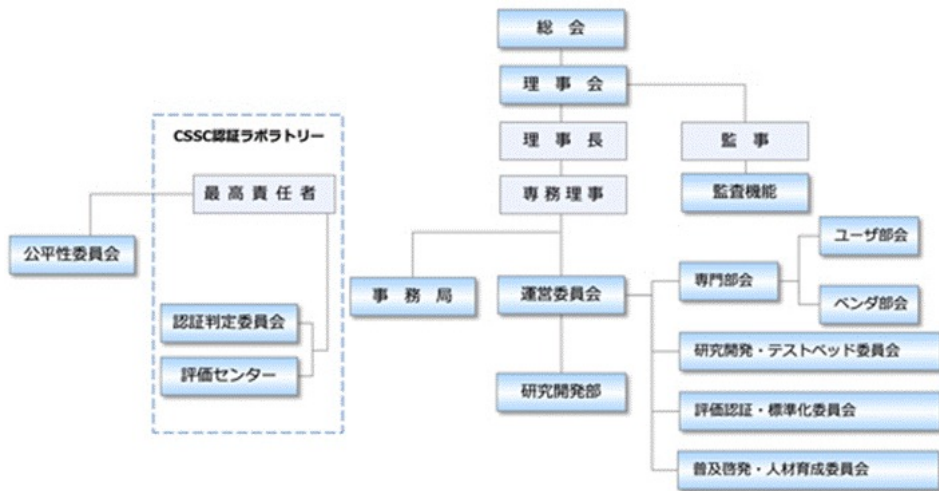
テストベッド（CSS-Base6）概要



<http://www.css-center.or.jp/>

CSSCの組織体制

理事長 高橋信
(東北大学教授)



- ・ユーザ部会は、電力部会とビル準備部会を設置
- ・ベンダ部会は、教育部会、法制度部会、
防衛製品評価部会を設置
- ・電力部会は、電事連殿ご参加、
電力分野のサプライチェーンリスク対策を検討

役職	氏名	所属等
理事長	高橋 信	国立大学法人東北大学 大学院工学研究科 技術社会システム専攻 量子エネルギー専攻 (兼任) 教授
専務理事	渡部 宗一	イーヒルズ株式会社 取締役
理事	須藤 健次	アズビル株式会社 執行役員
理事	田中 良夫	国立研究開発法人産業技術総合研究所 執行役員
理事	佐々木 修	通研電気工業株式会社 理事 ソリューション推進事業部長
理事	油井 公義	株式会社トイックス 常務取締役営業本部長
理事	石井 秀明	株式会社東芝 特別嘱託
理事	石原 修	株式会社日立製作所 シニアエキスパート
理事	諏訪 啓	三菱電機株式会社 デジタルイノベーション事業本部 DI戦室IT・ セキュリティガバナンスユニット ユニット長
理事	森 浩生	森ビル株式会社 取締役 副社長執行役員
顧問	渡辺 研司	名古屋工業大学 教授
顧問	小林 和真	奈良先端科学技術大学院大学 客員教授 京都産業大学 情報理工学部 特定任用教員 (教授)
顧問	稲垣 隆一	稲垣隆一法律事務所 弁護士
監事	丸山 満彦	PwCコンサルティング合同会社 パートナー 執行役員
事務局長	村瀬 一郎	技術研究組合制御システムセキュリティセンター

CSSCの活動目的と事業内容

- 1 ユーザ企業の制御システムセキュリティ確保
- 2 組合員における制御システムセキュリティ確保に向けた取組の向上
- 3 制御システムセキュリティ確保に向けた技術の蓄積

- ・ 制御システムの高セキュア化の研究開発
- ・ 制御システムや制御機器の評価認証
- ・ 制御システムセキュリティの普及啓発人材育成

ユーザ連携事業
組合員と連携し、
ユーザ企業の制御システムセキュリティ確保のための検討（電力部会、ビル部会、ベンダ部会等）

附帯事業
研究開発成果をもとに、
国や民間企業等に対し、
関連サービスを提供
（教育、セキュリティ
検証、リスクアセスメント、
評価認証等）

研究開発事業
制御システムセキュリティ確保のための技術の蓄積・研究
（ロボットセキュリティに向けた検討、研究インフラの研究等）

研究開発
教育
ペネトレーションテスト
リスクアセスメント
評価認証

テストベッド（CSS-Base6）概要



<http://www.css-center.or.jp/>

模擬システム

ビル模擬システム



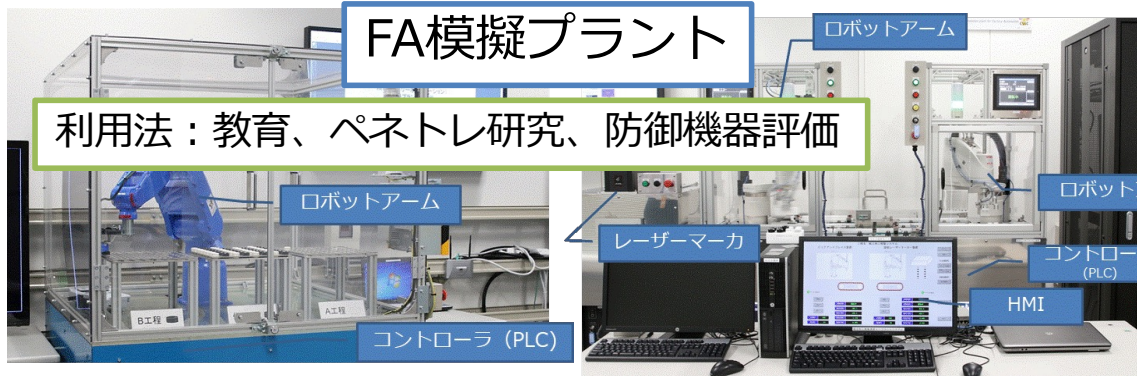
利用法：教育、ペネトレ研究、防御機器評価

定圧プラント



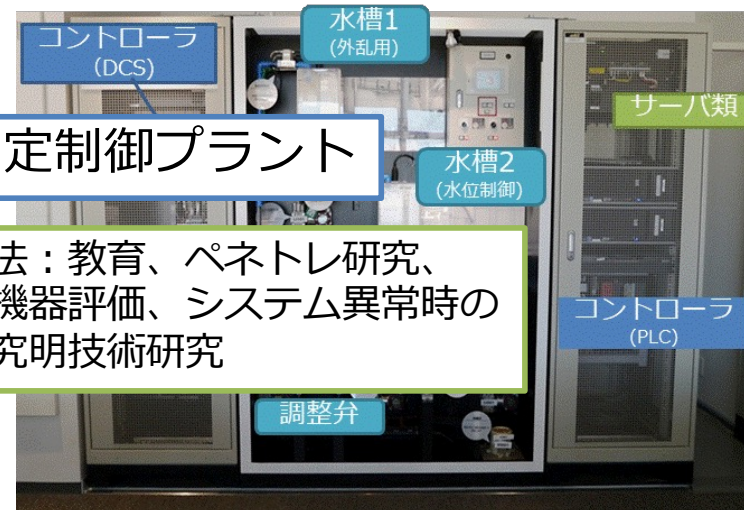
利用法：教育、ペネトレ研究、防御機器評価、困難環境下のロボット技術研究

FA模擬プラント



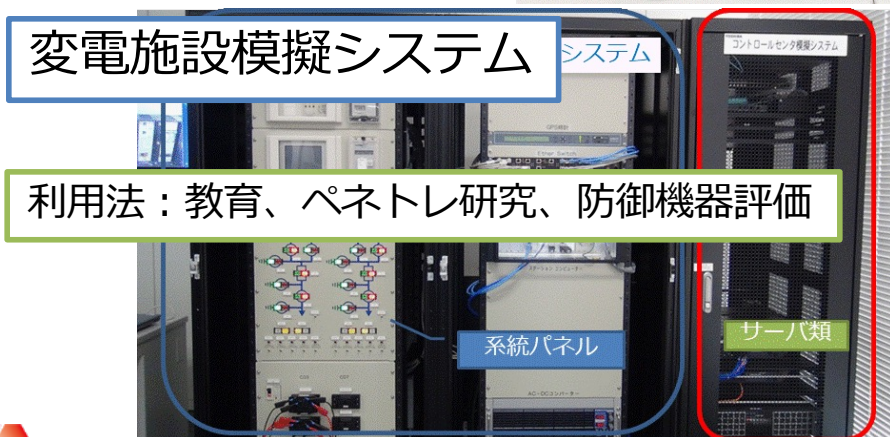
利用法：教育、ペネトレ研究、防御機器評価

水位一定制御プラント



利用法：教育、ペネトレ研究、防御機器評価、システム異常時の原因究明技術研究

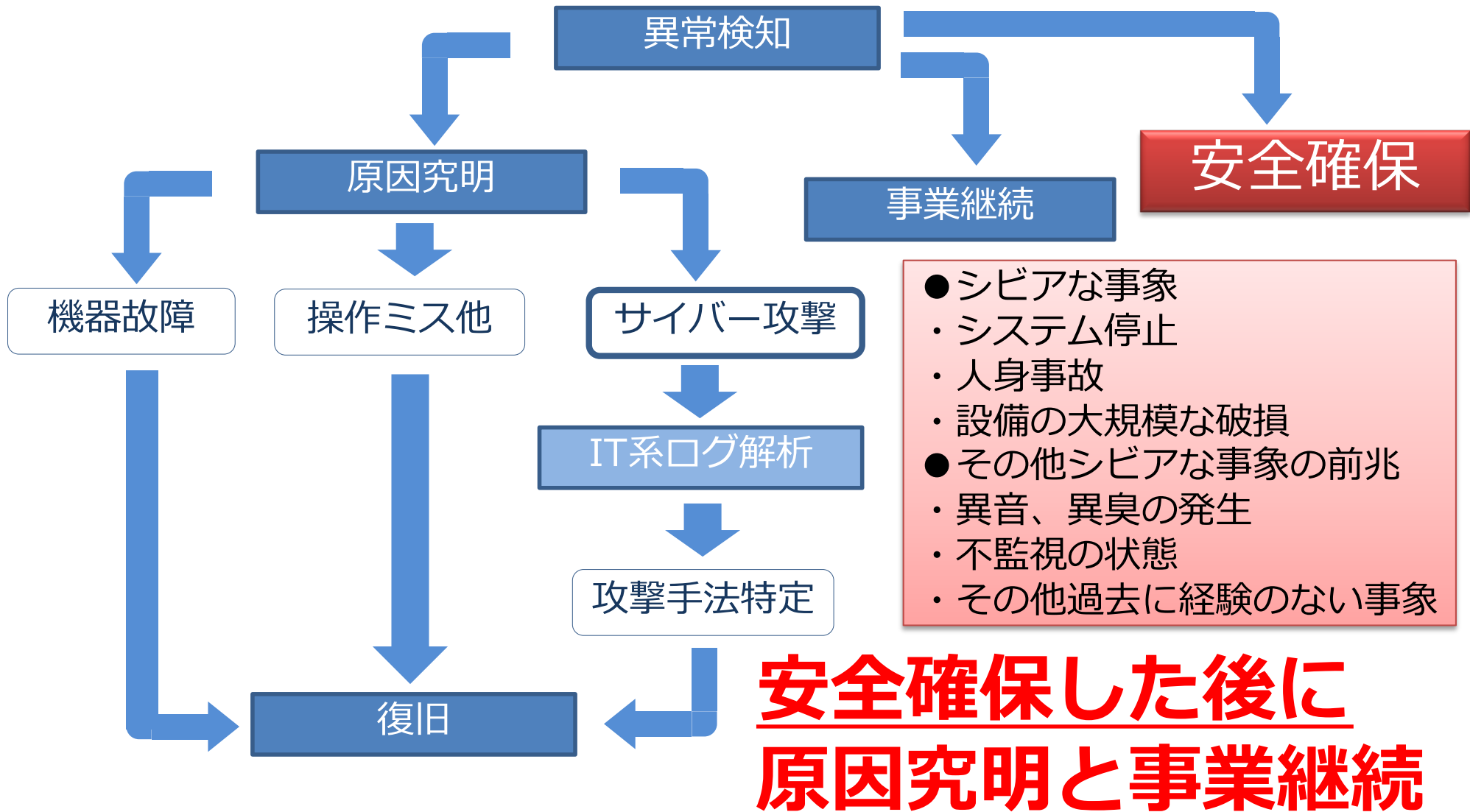
変電施設模擬システム



利用法：教育、ペネトレ研究、防御機器評価

制御システムセキュリティの対策について

制御システムの緊急対応プロセスの全体像



対策のポイント

1. 安全対策

- 制御システムにおいても安全確保が最優先であり、安全確保を行った上で原因究明と事業継続を実行
- 一瞬の判断により生命身体の安全や機器の大規模の物理的損傷が伴う場合、複数人での意思決定は不可能であり、1人に権限を集約することも必要

2. 制御システムおよび情報システム異常時の対応

- サイバー攻撃を前提とした対応を行うことは困難であり、ランサムウェアを除いて原因究明の結果としてサイバー攻撃であることが判明
- セキュリティパッチを当てることは不可能な場合が多い
- システム障害時には、機器故障・誤操作を中心に原因究明を行い、サイバー攻撃の可能性も考慮
- ウィルス・マルウェアに感染した場合機器に影響がない場合、様子を見ることも一案

3. 原因峻別のためのログ収集と分析

ログは、攻撃シナリオをユーザ企業自身が作成し、それに沿ったログの収集と分析を行うことが必要。攻撃シナリオを大別すると、USBメモリ等外部記憶媒体からのマルウェア感染、サーバールームでの超小型コンピュータ設置、イントラを介した不正アクセス、不正操作・誤操作、他通信回線や外部電源回線の物理的破壊、クラウド等外部リソースの誤設定等

4. ランサムウェア対策

- 制御システムに異常がなくても情報システムのサーバをランサムウェア化すれば可用性を侵害可能
- 対策は、バックアップの定期的な取得とデータの可読性確認を含むリストア訓練およびリストアデータによる稼働訓練（身代金は払わない）

制御システムセキュリティ対策は、ユーザが主役であることを認識する。（防御機器はユーザ側で設定が必要、攻撃シナリオはユーザしか考えられない）

サイバー攻撃に係る原因究明ノウハウ

1. 予兆の確認

ウィルスやマルウェア感染の場合、他企業でも感染しているウィルス等の動向を把握

- マルウェアの特徴
- 感染経路（添付ファイル付電子メール、ウェブサイト経由、ファイル共有経由、外部記憶媒体）

2. ログの確認

制御系データ（センサーデータ、操作ログ、アクチュエータのデータ等）とIT系ログの横断的分析

- 計測データ異常時以前にIT系ログ（ファイヤーウォール、通信機器やOSのログ等）にて異常があるかを分析
- 攻撃シナリオに沿った分析（外部記憶媒体や持ち込みPC、イントラ経由、不正操作等）

3. 他の要因では想定できない不審な動き

- 計測データの異常より前にIT系データの異常がある場合
- 機器故障や操作ミスでは考えられない制御系データの変動
- 台帳にない機器の接続
- 機器の意図的な破壊
- 設定データや計測データ等の不審なアップロード
- 機器交換しても繰り返し異常発生
- 操作ミスが無いにもかかわらず不審なセンサーデータの変動
- VPN機器やRDP機器のパスワード漏洩 他

正常時における制御システム全体の振る舞いを認識し異常時との比較実施が重要

CSSCの制御システムセキュリティ教育

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 [何れも日数、教育内容等は相談可能です。](#)
- 5) 評価認証（詳細省略）

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

東北大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

東北大の場合最大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
50分	制御システムセキュリティに係る法制度
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

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

東北大。

4. 日時

別途御相談。

5. 費用等

ご相談。

6. 人数

最大30人程度。

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	210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）
16:30	50分	制御システムにおける緊急時の対策
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）

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

数百万円から

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) 東北大の場合

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

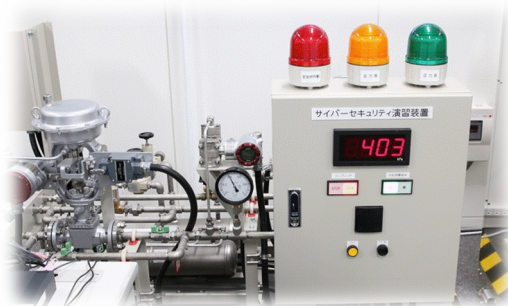
1日目			
9:30	9:40	10	オープニング
9:40	10:45	65	制御システムセキュリティの脅威と対策の基礎
10:55	12:00	65	制御システムセキュリティの対策の詳細
昼食			
13:00	14:05	65	セキュリティ検証の概要
14:15	16:00	105	ペネトレーションテストの概要
16:15	17:30	75	ペネトレーションテストの活用方法
2日目			
9:15	10:30	75	ペネトレーションテスト実習(1)
10:45	12:00	75	ペネトレーションテスト実習(2)
昼食			
13:00	14:15	75	ペネトレーションテスト実習(3)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

情報処理安全確保支援士特定講習
制御システムセキュリティ教育講習
(入門編)

講習の概要

特徴

- 制御システム及び制御システムセキュリティに関する座学を実施。前提知識の解説も行うため、これまで制御システムに関わったことがない方も理解が深まる講習
- CSSC所有の模擬プラントを受講者自らで操作、監視する演習を実施（仮想マシン上ではなく、実際のプラントを使用して演習を実施します）
- 演習はグループディスカッションを取り入れた参加型の講習
- 重要インフラ等のリスクアセスメントの監査員やセキュリティ検証のテスター経験者が講師を担当



ガス模擬プラント



変電模擬プラント



水位一定制御プラント

講習の概要

過去の受講者の感想(抜粋)

- 制御系システムセキュリティに関する近年のインシデント事例や必要性などを学ぶ良い機会となった。
- インシデント対応は頭の中のイメージでしかなかったのですが、実体験することで、ここまで御膳立てされていても特定や確認に時間と労力がかかることがわかったのが非常に有意義だった。
- 実際のインシデント・サイバー攻撃に近い状況を体験することができ、非常に有意義な教育だと感じた。
- 演習を通してインシデントの経緯を追うという貴重な体験だった。机上の講義についても、あまり深掘りできていなかったインシデント案件の解説を聞いた事が非常に有益だった。
- 最近の動向を紹介してもらったのは大変有益だった。

講習の概要

講習内容

- 制御システムの概要と脅威、セキュリティ対策動向に関する座学を実施。
- その後、模擬システムを使用した参加型のインシデント対応演習を実施する。
- グループディスカッション、発表を通じて制御システムの実情と脅威に関する基礎を習得する。

到達目標

- 制御システムの概要と、制御システムに使用されている代表的な機器や構成を理解する。
- 国内外の制御システムへのサイバー攻撃の事例を理解する。
- 制御システムへの攻撃シナリオを体験し、調査・分析・対策の策定を理解する。

講習の概要

1. 制御システムの脅威と対策

【内容】

制御システムの構成（制御システムとは、DCSとPLCの違い、センサ、アクチュエータ）、制御システムの歴史と背景、各分野の特徴を学習する

制御システムセキュリティを理解するために、制御システムへのサイバー攻撃の歴史を学習する。また、制御システムのセキュリティ対策の基本を国内外の制御システムセキュリティ対策に関するガイドラインや標準、規格を参照しつつインシデント発生時の復旧、事象対応の流れについて、情報系との違いを中心に学習する。

2. 模擬システムによる実機演習①（変電所模擬システム）

【内容】

変電所模擬システムを使用し、攻撃シナリオに対する、調査、分析、報告をグループ演習で実施する。また、それぞれの調査結果の発表を行い、ディスカッションする。

実際の変電所模擬システムを使用し、操作を行う。

変電模擬プラント



講習の概要

3. 模擬システムによる実機演習②（ガス模擬プラント）

【内容】

攻撃者の視点に立ち、模擬攻撃を行う演習を体験する。攻撃者の目線で模擬システムに対してどんな攻撃が実施できるか検討し、ディスカッションの上発表を行う。

実際のガス模擬プラントを使用し、操作を行う。



4. 模擬システムによる実機演習③ （プロセスオートメーションシステム）

【内容】

化学プラントを利用し、各グループごとにインシデントに対するログ調査を実施する。

実際のプロセスオートメーションシステムを使用し、操作を行う。



CSSCのペネトレーションテスト

CSSCのペネトレーションテストの特徴

対象

1. 制御システムや制御機器（スマートメーターシステムや関連機器を含む）を対象
2. ブラックボックステストを基本とし、あらゆるプロトコル種別を対象
3. 有線イーサネットだけではなく、無線系やシリアル通信も対応可能
4. IPv4だけではなくIPv6、産業用イーサネット通信プロトコルの検証にも対応可能

検証手法の特徴

1. CSSCが有する検証技術により可能な範囲で脆弱性を抽出する
2. 脆弱性やパラメータチューニング、組み合わせなど独自のノウハウを用いて実施
3. 想定脅威を再現するために、必要に応じて保有ツールのカスタマイズやツールの新規製作を実施し
4. ネットワークを介したテストとともに耐タンパー関連テストも実施可能

その他

1. ツールベンダーとのコネクションを有しており、対応プロトコル追加等についても正常データのエミュレーションや検証パケット作成に柔軟に対応
2. 発見した脆弱性については複数の対策案を合わせて提案
3. WebサイトやWebアプリケーション等への対応も可能

○有線系のツールと特徴

1. 有線系のツールは、nmapやmetasploit等のフリーソフト、nessusやBrekingPoint等の商用ソフト、自作ツールを保有
2. 正常な情報系、制御系プロトコルのトラフィックを模擬しつつ、各種サイバー攻撃トラフィックのエミュレーションをおこなうことで、CPU使用率の頭打ちなどによる処理落ちなど現実的な検証が可能

○無線系のツールと特徴

1. 無線系のツールは、パケットキャプチャドングルやスペクトラムアナライザ 評価用の無線デバイスのカスタマイズ品を保有
2. 電波暗箱を利用し、無線設備規則等に縛られないテストも実施可能

事前準備

1)脅威の特定

御社とCSSCで打ち合わせを重ね、脅威の特定を行います。
脅威の特定とは、「制御システムにおいて、何が発生すると問題か」に関して、お互いの認識を共有することです。
同時に、攻撃方法（主として物理攻撃の関与の度合い）に関する議論もさせていただきます。

2)検証範囲の特定

脅威の特定の結果を踏まえ、検証範囲を明確化します。
一般には、システム構成図概要版をもとに、検証対象となるサブシステムの特定を行います。

3)検証環境構築

検証範囲の明確化終了後に、検証環境構築を行います。検証環境は御社に構築頂くか、すでに構築されているテスト用等の検証環境を利用することも一般的です。

検証作業

1)事前検証1（既存ツールを用いた検証）

Nmap、Nessus、Metasploitを用いて情報収集を行います。並行して開示情報から、システム構成・チップ情報等を収集します。さらには、これらの情報収集により得られたシステム構成図を作成します。

2)事前検証2（CSSC独自のプロトコル検証）

PPS限界測定、TCP header smurf、TCP不正pktサイズ攻撃、ARP spoofing、マルチキャスト攻撃等による検証を行います。さらには、制御ネットワーク部分の packets をモニタリングし、プロトコルやパラメータの推定等を行います。

3)攻撃シナリオの検討とツールの製作

1)の脅威を前提として、2)の結果を用いて攻撃シナリオを検討致します。必要に応じて、ツールの製作を行います。

4)本検証作業

3)で作成した攻撃シナリオに関して、検証作業を行います。脆弱性が発見できない場合、4)に戻り攻撃シナリオの検討とツールの製作を再度行います。

CSSCのリスクアセスメント

CSSCのリスクアセスメントのポイント

前提条件：

脅威シナリオとチェックリストをご提供します。

- 事業継続上の脅威の綿密な検討と脅威シナリオの詳細化
事業継続上の脅威をお客様毎に綿密に決定し、それらを発現させる脅威シナリオを詳細化します。
- 特に、制御システムの特徴である安全性に焦点を当てます。
- サイバー攻撃のみならず、施設の破損や誤操作等の制御システム異常全般を想定したシナリオを作成します。
- 公開情報または追加情報によるチェックリストの作成
上記の脅威シナリオに対するチェックリストを詳細に作成します。
- 近年の安全保障環境の劇的変化に対応したチェックリストを作成します。

1. 事業継続上の脅威の検討

○事業継続の脅威の想定案

電力制御システムにおける事業継続上の脅威は以下のように設定可能である。

- ① 安全や環境に及ぼす事態が発生する
- ② 信用失墜につながる事象が発生する
- ③ 関係者の業務量が著しく増加する事象が発生する

○攻撃シナリオとチェックリスト

添付資料（CSSSCのリスクアセスメント攻撃シナリオと解説資料ver2.8電力向け、CSSSCのリスクアセスメントチェックリストver2.8）参照。これをもとに、カスタマイズします。

2. 脅威シナリオの詳細化

項番	発生すると困る脅威	具体的事象
1	①発電所（例）にて安全や環境に及ぼす事態が発生する	中央制御室の機能がダウンする

下記の脅威シナリオを、「発生すると困る脅威」毎に、20程度を上限に作成

脅威シナリオ（例）
○USBメモリや外部持込PCからのウィルス感染 USBメモリから保守端末にウィルスが感染し、サーバを介して多数の監視制御端末がブルー画面となり、工場全体が不監視の状況となり工場全体をダウンさせる。
○超小型PCからの攻撃 超小型PCが中央制御室内のネットワークに装着され、工場内の主要なサーバにDoS攻撃を行い、監視制御端末から工場全体が不監視の状況となり操作員が工場全体をダウンさせる。
○情報系システムを介した攻撃 情報系システムの共有ファイルサーバへのランサムウェア感染を端緒として、多くのサーバや端末がランサムウェアに感染し、念のために工場内のすべての制御システムをダウンさせる。
○リモート接続端末を用いた攻撃 工場内のインターネットを介してVPN接続されているベンダの操作員が誤操作により、中央制御室内サーバや端末がウィルス感染し監視制御端末がダウンする。
○制御系ネットワークにおける不正操作 監視制御端末において、誤操作によりアプリケーションサーバのディスクが全消去され、制御システム全体をダウンさせる。
○無線LANに係わる攻撃 工場内の無線LAN接続による保守用ハンディターミナルのための正規のアクセスポイントに不正な端末が接続され、工場内の機器に接続された主要な通信機器にDoS攻撃を行い、監視制御端末から工場内の設備が不監視の状況となり、操作員が工場全体をダウンさせる。
○外部のインフラからの供給途絶による機能不全 工場の建屋への電源供給システムがマルウェア感染によりダウンし、工場全体がダウンする。
○安全系システムへの攻撃 (この事象には関係しない)
○バックアップシステムや予備品への破損 USBメモリから制御システムのバックアップ系のサーバにマルウェアが感染し、バックアップ系がダウンする。その後、正常系に対して同様の攻撃が行われ、制中央制御室の機能がダウンする。
○外部ネットワーク上のリソースの影響 工場内の機器のリモート監視システムの利用している汎用クラウドの仮想化ソフトが誤設定により、第三者がリモート監視システムにアクセス可能状態となり工場内の関連サーバがダウンし、結果的に中央制御室がダウンする。

3. チェックリストの作成と評価

公開情報とお客様から開示して頂いた資料をベースに脅威シナリオ毎のチェックリストを作成します。

チェックリストに対してはコメントを頂き、逐次反映することを想定しています。

また、資料とヒアリングによりチェックリストによる評価を行います。

4. 納品物

以下を納品します。

1. 事業継続上の脅威
2. 脅威を発現する脅威シナリオ
3. 脅威シナリオ毎のチェックリスト
4. 脅威シナリオ毎の現状の評価
5. 対策の方向性