サイバーセキュリティ演習

技術研究組合制御システムセキュリティセンター

201406

サイバー演習とは

- システムにおけるインシデント発生を想定したシナリオを設定し、関係者が参加して既存のマニュアルやルール、想定できる対応に関する課題を抽出する場

ポイント

✓組織に合致した目的の設定と関係者間での目的の共有
✓目的に沿ったシナリオの設定
✓**演習を通じた課題抽出**
✓演習成果の対策への反映

演習　≠　訓練

サイバー演習とは　–演習の種類-

目的による分類

1.セミナ　→認知徹底（教育）
2.ワークショップ　→議論や目的の説明
3.ゲーム演習→自由制御方式での対抗戦、新手法の発掘
4.机上演習　→議論を掘り起こす
5.通知訓練 →情報や体制アップ指示等の伝達訓練の事
6.機能演習　→組織機能の検証評価
7.フルスケール演習　→総合演習の事

演習制御方式による分類

・シナリオ制御
・攻撃守備

・研究的演習
　→機能演習や机上演習の前準備として、セミナ、ワークショップ等から開始し、演習参加組織の演習概念や目的意義等のイメージ合わせを目的とする。
・机上演習
　→機能演習実施に向けた演習課題の抽出整理やシナリオイメージを固める事を目的とする。実組織関係者が参加。
・機能演習
　→実際の組織の指示判断系統機能を用いて模擬的に検証するための演習。

サイバー演習とは　–サイバー演習の種類-

目的 / 脅威	情報連絡	技術的対応	その他
IT障害	・IT障害発生時の社内外の情報連絡	・サイト間のホットスタート	・IT障害発生時のBCP発動
サイバー攻撃	・サイバー攻撃発生時の社内外の情報連絡	・標的型メールによるユーザの対応	・サイバー攻撃発生時のマスコミ発表内容
その他（自然災害や重要インフラの障害）	・停電発生時のシステム担当者を含む社内の情報連絡	・通信障害発生時の原因究明	・大規模震災発生時の情報システムへの影響検討

サイバー演習の内容（例）

■サイバー演習の事例

実施主体・名称	対象（参加者）	概要
NISC重要インフラにおける分野横断的演習 CIIREX（2006年-毎年）	**国内重要インフラ10分野**（情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流）	**重要インフラに対し分野横断的に影響を与える脅威**を想定し、各分野の対応力強化、**官民の情報連携**の推進、**重要インフラ防護対策**の向上などを目的としたサイバー演習。
米国DHS Cyber Storm I – VI (2006, 2008, 2010, 2011-12)	**官**（連邦/州政府/自治体）及び**民間セクター**（主に重要インフラ事業者）、各分野の**ISAC**※等	官民のサイバーインシデントに対する準備・防護・対応強化のための演習。政府の**意思決定・調整機能**、**官民の情報共有機能**の検証等が目的。
欧州ENISA Cyber Europe (2010, 2012)	EU加盟国の関連省庁、CERT組織、情報機関等	**大規模なサイバー攻撃**に対する欧州諸国の対応強化のための**連携体制の構築**を目的とした演習。
米国FS-ISAC （金融分野のISAC） CAPP Exercise (2010)	金融分野関係者（金融機関、カード決済会社、代行サービス事業者、小売業者、企業財務、政府機関等）	支払いプロセスへの攻撃を想定した3日間のオンライン演習。参加者には演習後、**結果のサマリ、ベストプラクティス及びリスクマネジメントに関する推奨事項等**が記載されたレポートが配布された。

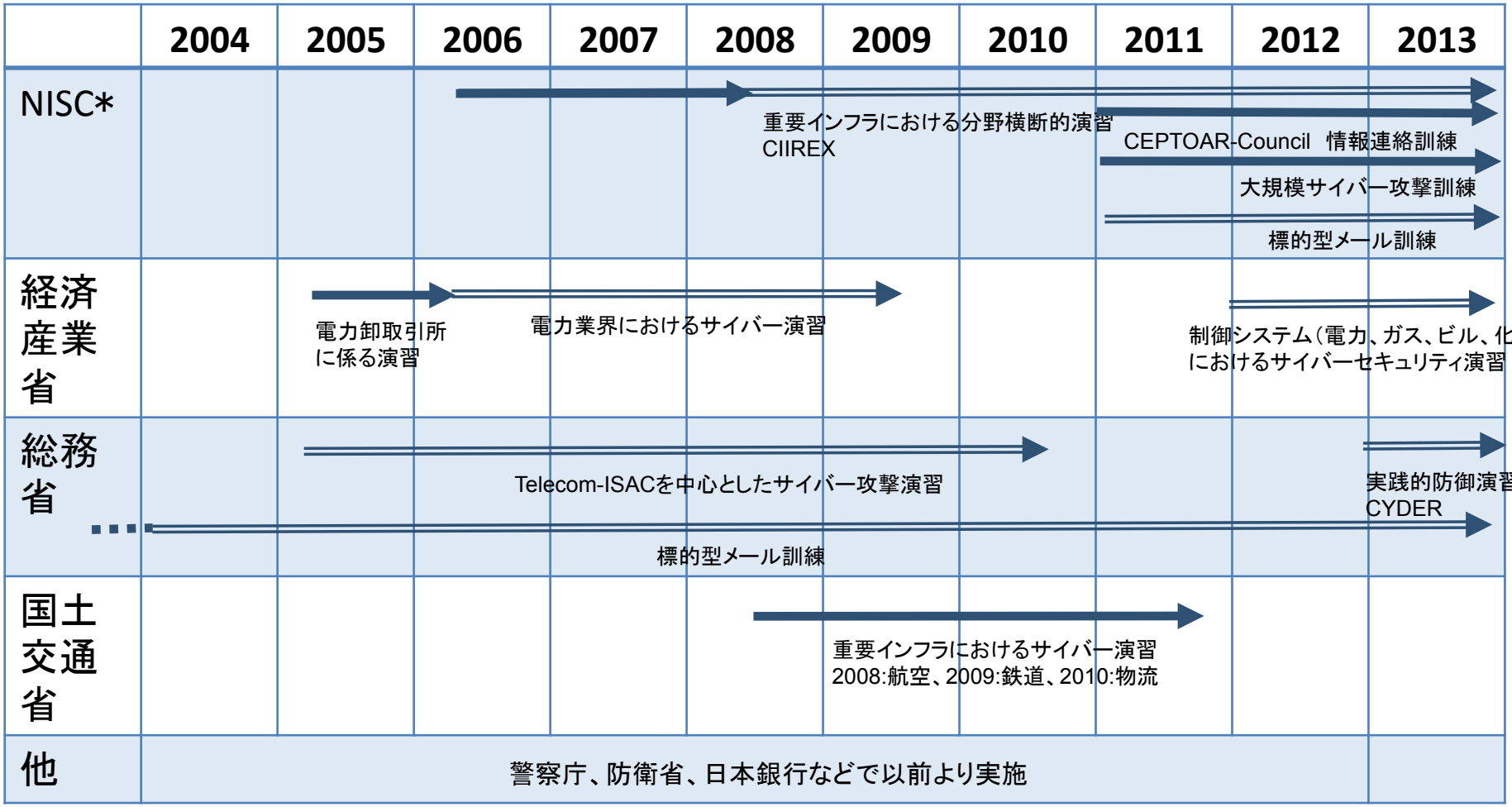
CIIREX (2009)

Cyber Storm III (2010)

Cyber Europe(2010)

出典：日NISC, 米DHS, 欧ENISA

■国内のサイバー演習の歴史的経緯



＊NISC： National Information Security Center、内閣官房情報セキュリティセンター
民間分野では、金融、通信においてはサイバー演習が常態化している

→ 机上演習
⇒ 機能演習

平成25年度サイバーセキュリティ演習の目的と特徴

【演習の目的】
- 電力分野、ガス分野、ビル分野、化学分野において、現場の担当者、技術者、関係するベンダ等が、制御システムにおけるセキュリティ上の脅威を認識し、セキュリティインシデント発生の検知手順や障害対応手順の妥当性の検証を目的とするサイバーセキュリティ演習を実施し、各分野の参加者における制御システムセキュリティにおける対策を中心とした知見の獲得を促す。

電力	• 業界団体、電力事業者（10社予定）、ベンダ（日立製作所）、事務局（CSSC）、事務局支援（三菱総合研究所）による実施体制 • 火力発電所制御システムの模擬システムを用いた演習を実施 • 最新の情報セキュリティ脅威動向等に係わる机上演習を実施
ガス	• 業界団体、ガス事業者（10社）、ベンダ（アズビル）、事務局（CSSC）、事務局支援（三菱総合研究所）による実施体制 • PCと通信機器、およびコントローラを組み合わせた模擬システムを用いた演習を実施 • 最新の情報セキュリティ脅威動向等に係わる机上演習を実施
ビル	• ビル事業者（森ビル等）、模擬攻撃者、事務局（CSSC）、事務局支援（三菱総合研究所）による実施体制 • 今後竣工されるビル等にも多く利用されるBA（Building Automation）システムを用いた模擬システムを用いた演習、及び攻撃ツール（Breaking Point）を用いた対戦型サイバー演習を実施 • 最新の情報セキュリティ脅威動向等に係わる机上演習を実施
化学	• 業界団体、化学工業事業者（4社）、ベンダ（横河ソリューションサービス、アズビル）、事務局（CSSC）、事務局支援（三菱総合研究所）による実施体制 • 2種類の化学プラントの模擬システムを用いた演習を実施 • 最新の情報セキュリティ脅威動向等に係わる机上演習を実施

平成25年度サイバーセキュリティ演習実施概要

	2014.1	2014.2	2014.3	参加者数
電力			火力▲ 3/6,7　広域▲ 3/24	全113名
ガス	1回目▲ 1/21,22	2回目▲ 2/24,25		全124名
化学			▲ 3/4	全51名
ビル	▲ 1/27			全68名

各分野において、業界団体、事業者、有識者、所管省庁、CSSC 等が参加

演習実施スケジュール（電力）

演習プログラム　　電力関係者参加者： 51名

時間	内容	場所
1日目		
13:00	式典（20分）	
13:20	机上演習（40分） ・制御システムセキュリティの動向説明（発生インシデント、国際規格等）	システム評価室
14:00	機能演習（90分） ・セキュリティインシデントの実機演習（侵入、発症）	模擬プラント室
15:30	休憩（20分）	
15:50	機能演習（75分） ・セキュリティ対策技術の実機演習（発症防止、侵入防御）	演習室（グループ毎に実施）
17:05	休憩（5分）	
17:10	機能演習（20分） ・セキュリティ対策技術の実機演習（検知技術） ・機能演習の振り返り	模擬プラント室
17:40	終了	

時間	内容	場所
2日目		
9:00	機能演習（30分） ・セキュリティインシデントの実機演習（Stuxnet） ・セキュリティ対策技術の実機演習（検知技術）	模擬プラント室
9:30	休憩（10分）	
9:40	机上演習（80分） ・セキュリティ設計グループ演習	前半：システム評価室 後半：演習室
11:40	意見交換会、有識者からの講評（30分）	システム評価室
12:10	挨拶（10分）	システム評価室
12:20	終了	

演習実施スケジュール（ガス）

演習プログラム（1日目）

時間	内容	場所	参加者		
			プレイヤ	プレイヤ以外	プレス
1日目					
13:00	挨拶（20分） 機能演習（デモ）（80分） ・機能演習の説明 ・シナリオ0（デモ・演習の流れや操作の理解）	システム評価室 模擬プラント			
14:40	休憩（10分）				
14:50	机上演習（60分） ・制御システムの概要と脅威 ・制御システムセキュリティの考え方とセキュリティ対策動向	システム評価室			
15:50	休憩（10分）				
16:00	機能演習（60分） ・機能演習の説明 ・シナリオ1（実機操作）	模擬プラント室			
17:00	有識者講評（30分）	システム評価室 または演習室			
17:30	終了				

※　1回目の演習後アンケートを踏まえ、2回目はデモを15分短縮し、机上演習を15分延長（75分）に変更

演習実施スケジュール（ガス）

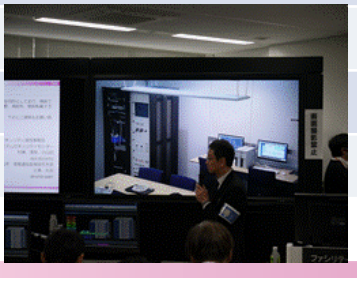
演習プログラム(2日目)

時間	内容	場所	参加者		
			プレイヤ	プレイヤ以外	プレス
2日目					
8:55	各種連絡(5分)	システム評価室			
9:00	機能演習(210分) (実機操作) ・シナリオ2～5	模擬プラント室			
12:30	休憩(30分) ※昼食	システム評価室			
13:00	個社毎の議論、有識者の個別講評(60分)	システム評価室 演習室			
14:00	意見交換会、有識者の全体講評(20分)	システム評価室			
14:20	挨拶(10分)	システム評価室			
14:30	終了				

演習実施スケジュール（ビル）

演習プログラム

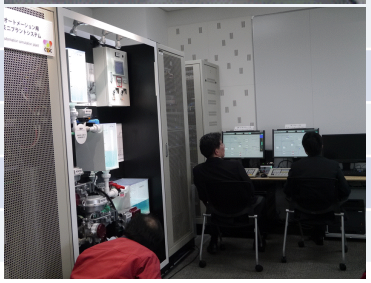
時間	内容	場所	参加者		
			プレイヤ	プレイヤ以外	プレス
09:00	参加者受付開始				
09:30	机上演習（90分）	システム評価室			
11:00	機能演習説明（60分） ・機能演習の説明 ・攻撃シナリオ0のデモ	模擬プラント室			
12:00	昼食	システム評価室			
13:00	機能演習1（90分）	模擬プラント室			
14:45	機能演習の解説（45分）	演習室CD		施設見学等	
15:45	機能演習2（対策実施後の演習）（45分）	模擬プラント室			
16:45	意見交換会	模擬プラント室			
17:30	懇親会	システム評価室			
18:30	解散（予定）				



演習実施スケジュール（化学）

演習プログラム

時間	内容	場所
13:00	挨拶（20分） **機能演習①-A（30分）** デモンストレーション（10分） ・制御システムの概要と脅威を動画と模擬プラントで体感 演習（20分） ・模擬プラントの説明 ・サイバーインシデントを想定する必要性の認識	システム評価室 模擬プラント室
13:50	机上演習（55分） ・CSSC紹介 ・化学プラント制御システムにおける脅威 ・制御システムセキュリティの考え方とセキュリティ対策動向	システム評価室
14:45	休憩（5分）	
14:50	**機能演習① -B（50分）**	模擬プラント室
15:40	**機能演習②（80分）**	システム評価室
17:00	休憩（10分）	システム評価室
17:10	意見交換会、有識者からの講評（40分）	システム評価室
17:50	挨拶（10分）	システム評価室
18:00	終了	



今年度のサイバーセキュリティ演習のまとめ

1. 模擬システムの利用
　各分野毎の模擬システムを用いた演習に関して、各分野担当者のインシデント発生時の対応を明示する点において有効。

2. 対策の提示
　セキュリティ上の脅威とともに対策に関して、多くの参加者が体感。

3. 模擬プラントへの攻撃
　一部分野にて模擬システムを攻撃することにより、実際のシステムの脆弱性が顕在化。

4. 意見交換会における情報交換
　有識者を混じえた意見交換会における情報交換により意識啓発および情報共有の有効性の認識。

【今年度演習の成果】

電力・ガス・ビル・化学の4分野における模擬プラントを活用した演習により、参加者は脅威と対策効果の体感を得ることができ、制御システムの情報セキュリティ確保を踏まえた事業継続を検討する上で有効と評価した。

【問題点】

参加者とシナリオとミスマッチが一部存在した。

サイバーセキュリティ演習の結果と今後の展開

【今年度演習の成果】

- 電力・ガス・ビル・化学の4分野における模擬プラントを活用した演習により、参加者は脅威と対策効果の体感を得ることができ、制御システムの情報セキュリティ確保を踏まえた事業継続を検討する上で有効と評価した。

【今後の展開】

- 各分野のニーズを踏まえ、シナリオや演習実施方法を継続的に改善する。
- 今年度作成した広報用ビデオや演習コンテンツ等を利用し、演習のさらなる普及を図る。
- 中小事業者等への展開や対象者層（経営層、計装エンジニア等）の拡大を念頭に置きつつ、模擬システムの活用と演習内容の充実に向けて、プログラム構成や開催数の見直しを行う。
- 演習成果を更に業界内に展開するために、ガイドライン作成等具体的な方策について引き続き各業界と共に検討を行う。