Vol.2016-DPS-166 No.10
Vol.2016-CSEC-72 No.10
2016/3/3

サイバー攻撃訓練システムにおける訓練シナリオ生成方法の提案

浅井健志[†1]　河内清人[†1]　祢宜知孝[†1]　泉幸雄[†1]

概要：近年，産業制御システムがインターネットと接続されることが多くなり，これに伴い当該システムに対するサイバー攻撃が増加している．そのため，監視員はサイバー攻撃を受けた際の適切な対応を訓練しておく必要がある．サイバー攻撃の活動内容は個々のシステムの構成に依存するため，監視員に対して訓練を行うには，訓練を行いたいシステムに即した攻撃活動をそれぞれ定義する必要がある．一方で，サイバー攻撃は頻繁に新しい事例が発生する．そのため，訓練を行うにあたり都度攻撃活動の定義作業が発生し，作業コストが増大するという課題がある．本稿ではこの課題の解決策として，訓練用の攻撃活動を攻撃のステップの単位で効率的に定義する方法を提案する。本提案では，訓練したいサイバー攻撃の攻撃活動と訓練対象のシステムの構成情報から，システム内の機器を用いて当該システム固有の活動を定義する．その際，訓練したいサイバー攻撃の特徴が顕著に表れたステップを必ず含むようにステップ間の整合を取る．

キーワード：サイバーセキュリティ，産業制御システム，訓練機，シナリオ生成

Scenario Generation Method for Cyber Security Trainer

TAKESHI ASAI[†1]　KIYOTO KAWAUCHI[†1]
TOMONORI NEGI[†1]　YUKIO IZUMI[†1]

Abstract: In recently years, Industrial Control System (ICS) system has connected to Internet and it increase cyber attacks to ICS. To reduce damage, the plant operator needs to learn and train appropriate action in case of cyber attacks. Activities of cyber attacks depend on the individual ICS configuration. Therefore, Trainer must define the adapted cyber attack scenario for each ICS to train plant operator. On the other hand, new cyber attacks occur continually, so trainer must very often re-define the scenario for each ICS. We propose a scenario generation method for cyber security trainer for this problem.

Keywords: Cyber Security, Industrial Control System, Trainer, Scenario Generation

1. はじめに

近年，産業制御システムを対象としたサイバー攻撃の事例報告が増加しており，その対策が急務となっている[1].

従来の産業制御システムは情報システムとは切り離されて設計されていたため，情報システムにみられるセキュリティリスクとは分離されて安全であるという認識があった．そのため，セキュリティについてはあまり考慮されていなかった[2]．しかし近年，産業制御システム外の管理システム/分析システムとの連携による生産性の向上や，監視/制御の集中化による省力化を目的に，情報システムとの接続や汎用機器/標準プロトコルの採用が進み，その結果として，情報システムにおけるセキュリティリスクが産業制御システムへ影響を及ぼすこととなった．特に，2010 年に発生したイランの原子力関連施設へのサイバー攻撃 Stuxnet[3][4][5]は，Windows の複数の脆弱性や USB デバイスを利用して感染を拡大し，最終的に標的のウラン濃縮遠心分離機を不正操作した．Stuxnet により，イランの核開発は何年も遅れたと言われており，被害は甚大である．この例に限らず，産業制御システムは重要社会インフラを担っていることが多く，ひとたびサイバー攻撃を受けると社会への影響が非常に大きい．Stuxnet の事件より，産業制御システムはサイバー攻撃と無縁である，産業制御システムとインターネットを切り離せば安全であるといった認識は間違いであることが知られることとなった．Stuxnet やその他の産業制御システムを対象としたサイバー攻撃の事件を受け，技術的な対策方法が多数研究されている[6][7].

一方で，サイバー攻撃がそのような技術的攻撃対策を回避してプラントに事故・異常事態を発生させた場合には，人的な対策，即ち，プラントでセキュリティの監視を行う監視員が適切なインシデント対応を取ることで，被害拡大の抑制・事態の収拾を図ることが求められる．

サイバー攻撃発生時にインシデントに対し円滑な対応を取るためには，監視員はその対処方法や手順を常に訓練しておく必要がある．そのような訓練を行う一手段として，実機のプラントを訓練用に余剰に構築することが考えられる．しかし，訓練のみの目的で実環境を構築することは，コストが現実的ではない．したがって，コストを抑えつつも可能な限り実システムに近い訓練環境を用意する必要がある．

そこで代替手段として，プラントの動作を仮想環境で模擬しその仮想環境上で訓練を行うという方法が提案されている[8][9]. サイバー攻撃の活動内容は個々のプラントのシステム構成に依存するため，監視員に対して訓練を行うには，訓練を行いたいシステムの構成に即した攻撃活動を，それぞれのプラントを模擬する仮想環境上で再定義する必

ⓒ 2016 Information Processing Society of Japan

要がある．

一方で，サイバー攻撃は頻繁に新しい事例が発生する[10][11]．したがって，訓練を行いたいサイバー攻撃事例が増加すればするほど，一つ一つの攻撃活動をその都度プラントの仮想環境上で再定義する作業が増大するという課題がある．

本稿では，以上のような課題を解決するために，訓練シナリオ作成にかかる作業コストを軽減するための方法，具体的には，訓練を行いたいサイバー攻撃事例の攻撃手順と，訓練対象となる産業制御システムのプラントの構成情報を基に，そのプラントの構成に即したサイバー攻撃のシナリオを生成する方法を提案する．

本稿は以下の構成である．2 章では関連研究について述べる．3 章で提案方法の説明を行い，4 章で考察し，5 章でまとめる．

2. 関連研究

サイバー攻撃検知訓練を目的として，仮想環境上で実環境に流れる正常な業務トラフィックを模擬するシステムの構築方法が提案されている[15]．そこでの提案では，実環境での障害解析やセキュリティ監査のために一般的に採取されているアクセスログを利用することで，実環境に新たにツールなどを常駐させることによる影響を排除している．さらに，採取したアクセスログは，暗号化による匿名化処理を行ったうえで，模擬用のデータを生成する．これにより，実環境に関する情報漏えいのリスクを軽減している．

しかし，複数の異なる産業制御システムのプラントに対し，同一のサイバー攻撃の訓練を行う場合は，そのプラント毎に模擬用のデータを生成する必要があり，多大な作業コストが発生するという課題がある．

例えばあるプラント企業が，保有する各プラントの監視員に対し同一のサイバー攻撃の訓練を実施したいとする．その際，各プランのト全てが同一のシステム構成を取るとは考えづらく，プラント内の装置の種類や数，またネットワーク構成等は異なると考えるのが自然である．さらにサイバー攻撃の活動内容は個々のプラントのシステム構成に依存するため，各プラント向けの訓練シナリオを定義するには，1 シナリオにつきプラント数分の作業コストが発生する．したがって，サイバー攻撃事例が増加すればするほど作業コストが増大する．

3. 提案方法

3.1 訓練システム

まず，本稿で対象とする訓練システムのシステム構成を図 1 に示す．訓練システムは，以下からなる．

- 教官用端末
  教官又は，訓練機メーカ(以下，単に教官と呼ぶ)が訓練シナリオを作成する，又は作成したシナリオを再生するため端末．
- 訓練者用端末
  訓練者が訓練時に操作する端末．
- プラント模擬用端末
  プラントの動作を仮想環境で模擬する端末．

訓練システムの概略フローを以下に示す．はじめに教官が訓練シナリオ生成機を用いて，訓練シナリオを作成する．訓練を開始すると，上記シナリオを入力として訓練シナリオ再生機が，プラント模擬用端末上の仮想環境内のプラントにサイバー攻撃がなされた際の挙動を再現する．訓練者は，訓練者用端末にある各プラント用の HMI などを利用して，仮想環境上のプラントや情報端末の操作を行い，サイバー攻撃被害時の対処方法や操作手順を習得する．本稿では，上記フローのうち訓練シナリオ生成機でのシナリオ生成方法について検討を行った．そこで，次節から訓練シナリオ生成機について説明する．

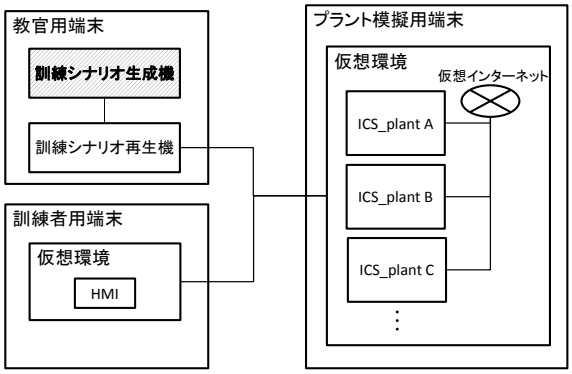

図 1 訓練システムのシステム構成

3.2 訓練シナリオ生成機

以下に，提案方法の概要を示す．教官は訓練シナリオ生成機に対し，訓練させたいプラントのシステム構成情報と，訓練させたいサイバー攻撃のシナリオ及び訓練シナリオ決定のための補助情報を入力する．訓練シナリオ生成機は，上記の情報を基に，それぞれのプラントに即した訓練シナリオを生成する．ここで，サイバー攻撃のシナリオとは，サイバー攻撃の一連の流れを，攻撃ステップの集合で表現したものである．また攻撃ステップとは，攻撃の活動単位のことであり，その例としては，感染や内部調査，不正通信等である．訓練させたいサイバー攻撃のシナリオを入力する際，教官は，各攻撃ステップに対しプラントを模擬する仮想環境上で必ず再現する攻撃ステップ(以下，必須ステップ)とオプションで再現する攻撃ステップ(以下，オプションステップ)のどちらかを指定する．必須ステップは，訓練者に訓練させたいサイバー攻撃の特徴が顕著に表れた攻撃ステップであり，この必須ステップを訓練者に体験させ

ⓒ 2016 Information Processing Society of Japan

ることを以て，元の攻撃シナリオの訓練を行ったとする．以降では，サイバー攻撃のシナリオに対して，必須ステップ/オプションステップの指定を行ったものを基本攻撃シナリオとし，基本攻撃シナリオを仮想環境上で実行するために，訓練対象のプラント内の機器名を用いて再定義したものを訓練シナリオとする．

訓練シナリオ生成機は，必須ステップを必ず含み，オプションステップを，訓練対象のプラントの構成に沿ったオプションステップへ適宜修正･代替しシナリオを生成する．これにより，構成情報が異なるシステムに対しても，サイバー攻撃の特徴が顕著に表れた攻撃ステップを含む意味で同一の訓練シナリオを適用することが可能となる．

3.3 訓練シナリオ生成機のシステム構成

提案する訓練シナリオ生成機のシステム構成を図 2 に示す．訓練シナリオ生成機は，
以下の機能ブロックからなる．

- システム構成入力部
  訓練対象となるプラントの構成情報の入力を受け付ける入力インタフェース．
- シナリオ入力部
  基本攻撃シナリオの入力を受け付ける入力インタフェース．
- シナリオ生成部
  訓練対象となるプラントの構成情報と，基本攻撃シナリオとから，訓練シナリオを生成する．サブ機能ブロックとして，判定部，補完部，出力部を備える．判定部は，各攻撃ステップが実行可能か否かを判定する．補完部は，オプションステップが実行不可の場合に，その代替ステップを生成する．出力部は，訓練シナリオを出力する．
- 情報記憶部
  機器の機能を示す機能情報と攻撃ステップの分類を示す攻撃分類情報とオプションステップの修正･代替する際に使用する前提ステップ判定情報を記憶する．これらの情報は，シナリオ生成部が適宜参照し利用する．また，教官が過去に入力したデータを保存しておき，後に流用する場合もある．

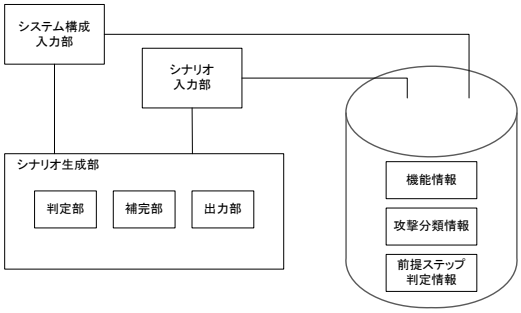

図 2 訓練シナリオ生成機のシステム構成

3.4 訓練シナリオ生成機の動作概要

次に，訓練シナリオ生成機の動作概要を図 3 のフローチャートを用いて説明する．なお，ここでの説明で用いる訓練対象のプラントのシステム構成は，図 4 に示したものとする．

まず，ステップ 1 において，教官はシステム構成入力部により，訓練対象となるシステムの構成情報とネットワーク構成情報を入力する．図 4 の例では，訓練対象システムには，ネットワーク 1 とネットワーク 2 が存在し，ネットワーク 1 には，操作装置 1 と操作装置 2 が接続され，ネットワーク 2 には，操作装置 2，コントローラ，制御対象装置 1，制御対象装置 2 が接続されている．教官は，システム構成入力部より，訓練対象システムに存在する機器名を入力し，入力した各機器名に対して，情報記憶部に事前に記憶されている機能情報の機能のリスト(表 1)から，適切な機能の選択を行う．これにより，訓練シナリオ生成機は機器名と機能との対応付けが行える(表 2)．また，ネットワーク構成情報については，ネットワーク名と当該ネットワークに接続された機器の機器名を入力する(表 3)．教官がステップ 1 を実行した結果，訓練シナリオ生成機は表 2 及び表 3 を内部に保持し，これらはステップ 3 で使用する．ここで，表 2 及び表 3 を情報記憶部に保存しておくことで，本訓練対象のプラントに新規のシナリオを追加したい場合に，本ステップを省略することができ作業コストを低減することができる．

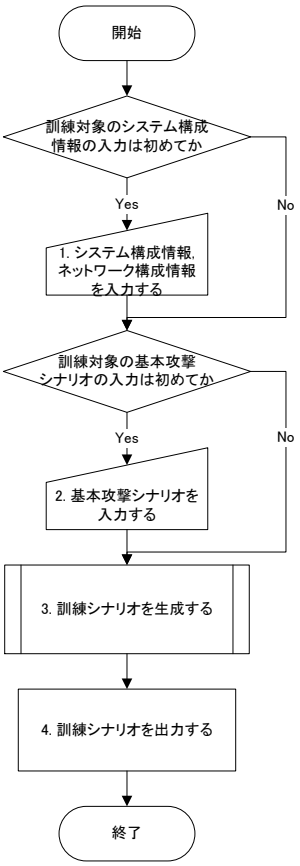

図 3 訓練シナリオ生成機の動作を示すフローチャート

ⓒ 2016 Information Processing Society of Japan

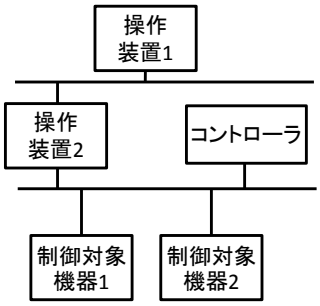

図 4 訓練の対象となるプラントの構成例

表 1 機能情報の例

No.	機能(要素)	機能(要素)の説明
1	HMI	監視員がプラントの操作・監視を行うための端末
2	EWS	監視員が制御プログラムの作成と PLC へのダウンロードを行う端末
3	PLC	制御プログラムを実行しセンサやアクチュエータの制御・情報収集を行う機器
4	OA-PC	事務用 PC
・・・	・・・	・・・

表 2 システム構成情報

No.	機器名	機能(要素)
1	操作端末 1	HMI
2	コントローラ	EWS
3	制御対象機器 1	PLC
4	制御対象機器 2	PLC
・・・	・・・	・・・

表 3 ネットワーク構成情報

No.	NW 名	接続された機器 1	接続された機器 2	接続された機器 3	・・・
1	NW1	操作端末 1	コントローラ	―	・・・
2	NW2	操作端末 1	コントローラ	制御対象機器 1	・・・

次に，ステップ 2 において，教官はまずシナリオ入力部により，訓練者に訓練させたい内容であるサイバー攻撃のシナリオを入力する．その際教官は，各攻撃ステップに対し，攻撃者による攻撃活動の分類(表 4)と，攻撃元及び攻撃対象となる機器の機能情報を選択し，これらの対応付けを行う．さらに，教官は，一連の攻撃ステップの中から，訓練者に訓練させたいサイバー攻撃の特徴が顕著に表れた攻撃ステップを指定する．ここで指定した攻撃ステップは，訓練対象システム個々のシステム構成に沿った訓練シナリオを作成する際に，必ず再現される攻撃ステップとなる．例えば，表 5 に示す攻撃ステップのうち，No.4 の EWS から PLC に対する不正通信が，訓練者に訓練させたいステップであるとすると，No.4 の攻撃ステップを必須ステップに設定する．教官がステップ 2 を実行した結果，訓練シナリオ生成機は基本攻撃シナリオ(表 5)を内部に保持し，ステップ 3 で使用する．ここで，基本攻撃シナリオを情報記憶部に保存しておくことで，入力した基本攻撃シナリオを新規のプラントに適用したい場合に，ステップ 2 を省略することができ作業コストを低減することができる．

表 4 攻撃分類の例

No.	攻撃分類
1	感染
2	不正通信
3	内部調査
・・・	・・・

表 5 基本攻撃シナリオの例

攻撃ステップ No.	攻撃分類	どこから(機能)	どこへ(機能)	必須
1	感染	―	OA-PC	No
2	感染	OA-PC	HMI	No
3	感染	HMI	EWS	No
4	不正通信	EWS	PLC	Yes

次に，ステップ 3 において訓練シナリオの生成を行う．生成はシナリオ生成部で行う．本ステップの処理フローについては後述する．

最後に，ステップ 4 において訓練シナリオ生成機は生成した訓練シナリオを出力し，シナリオ生成処理を終了する．

3.5 訓練シナリオの生成

ステップ 3 のシナリオ生成部における訓練シナリオの生成方法について説明する．フローチャートを図 5 に示す．なお，3.4 と同様に，ここでの説明に用いる訓練対象のプラントのシステム構成は，図 4 に示したものとする．シナリオ生成部の動作の骨子は以下である．シナリオ生成部は，教官から入力された基本攻撃シナリオに基づき，訓練対象のシステムの構成の機器を用いて当該システム固有の攻撃シナリオを出力する．その際，基本攻撃シナリオ中で「必須」に指定されたステップを必ず含むようにステップ間の整合を取る．

ⓒ 2016 Information Processing Society of Japan

3.5.1 必須ステップに対する処理

まず判定部が，表 5 から必須ステップを探索する．必須ステップが見つかると，表 2，表 3 から以下の条件で以て当該ステップが実行可能かを判定する．

1. 登録された攻撃ステップの，攻撃元となる機器の機能と攻撃先の機器の機能が存在していること．
2. それらの機能が，ネットワーク上で互いに接続されていること．

例えば必須ステップとして，「HMI から EWS への感染」を設定したとする．図 4 のシステム構成では，HMI 端末である操作装置 2 と，EWS 端末であるコントローラが存在し，これらは互いにネットワーク 2 を介して接続されている．そのため，本ステップは実行可能と判定される．別の例として，「OA-PC から HMI への感染」を設定したとする．しかし，図 4 のシステム構成には OA-PC が存在しないので，本ステップは実行不可であると判断される．判定した攻撃ステップが実行可能な場合は，当該の攻撃ステップ内の機能を教官が入力した機器名に置き換えて最後に出力する訓練シナリオ(表 7)に登録する．必須ステップが実行不可な場合は，処理を終了する．

3.5.2 前提ステップに対する処理

次に，必須ステップを実行する上で前提となるステップ(前提ステップ)をオプションステップの中から探索する．例えば，必須ステップとして，「EWS から PLC への不正通信」を設定したとする．本ステップを実行するには，それ以前に EWS へマルウェアが感染している必要がある．したがって，前提ステップは「XXX から EWS への感染」となる．この例のように，予めある攻撃分類に対応した前提ステップの攻撃分類，例えば表 6 の前提ステップ判定情報を情報記憶部に保存しておくことで，前提ステップの探索が可能となる．前提ステップが見つかると，必須ステップの場合と同様に前提ステップが実行可能かを判定する．実行可能な場合は，攻撃ステップ内の機能を機器名に置き換えて訓練シナリオに登録する．しかし，XXX が存在しない場合若しくは存在してもネットワークを介して接続されていない場合や，そもそも基本攻撃ステップに EWS へ感染するという前提ステップが存在しない場合は，必須ステップを実行するために前提ステップの内容を修正/追加する必要がある．その場合は，補完部が前提ステップの修正/追加を行う．攻撃シナリオとしては必須ステップが実行できればよいので，前提ステップへの要求は，必須ステップよりも前段において，前提ステップの結果さえ実行できればよい．表 5 を例にとると，攻撃ステップ No.3 は「HMI から EWS への感染」である必要が無く，単に「EWS へ感染」という結果さえあればよい．そこで例えば，システム内の機能を介すのではなく「USB 端末を介して EWS へ感染する」など，直接対象へ感染させるステップに修正する．前提ステップを実行するための機能が訓練対象のシステムに存在しない，又はネットワーク上で接続されていない場合は，前提ステップを上記に代替する．基本攻撃ステップに前提ステップが存在しない場合は，新規に「USB 端末を介して EWS へ感染する」を追加する．その後，攻撃ステップ内の機能を機器名に置き換えて訓練シナリオに登録する．前提ステップの訓練シナリオへの登録が完了した後は，全ての必須ステップの判定を完了したかを確認し，完了した場合はオプションステップの判定へ進み，未完了の場合は，必須ステップの判定へ戻る．

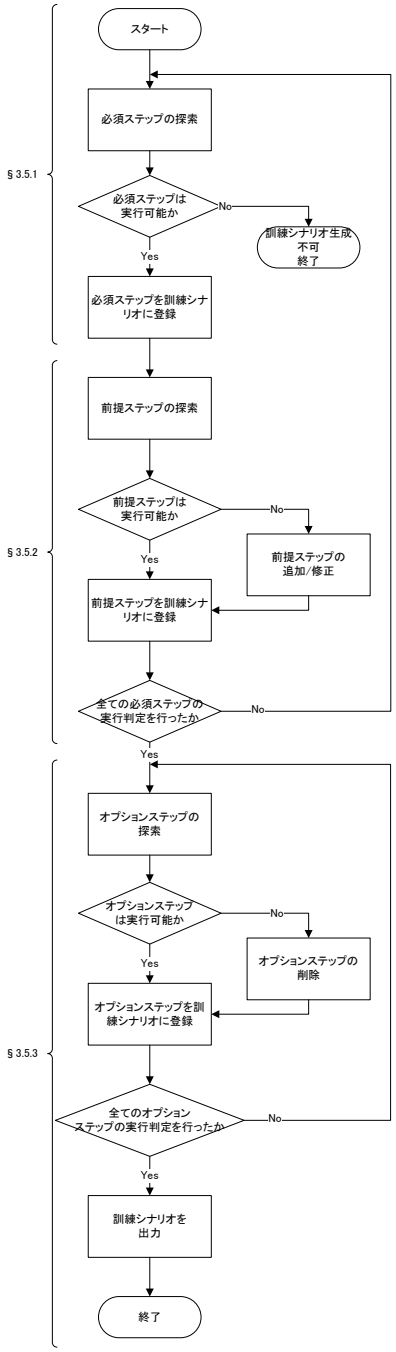

図 5 訓練シナリオ生成のフローチャート

ⓒ 2016 Information Processing Society of Japan

3.5.3 オプションステップに対する処理

次に，実行可能か判定を行っていないオプションステップを探索し判定を行う．実行可能な場合は，攻撃ステップ内の機能を機器名に置き換えて訓練シナリオに登録する．実行不可な場合は，補完部によりオプションステップを消去する．消去する理由は以下である．オプションステップが実行不可と判定される条件は,「前提ステップを実行するための機能が，訓練対象のシステムに存在しない場合」に対応するために前提ステップを修正し，後段のオプションステップとの整合が取れなくなった場合である．訓練シナリオとしては，必須ステップと前提ステップとの整合で十分であり,本オプションステップを実行する必要性が無い．そのため，本オプションステップは消去する．最後に，訓練シナリオを出力する．

表 6 前提ステップ判定情報の例

必須ステップの攻撃分類.	必要となる前提ステップの攻撃分類
不正通信	感染
・・・	・・・

表 7 訓練シナリオの例

攻撃ステップ No.	攻撃分類	攻撃元 (機器名)	攻撃対象 (機器名)
1	感染	－	OA-PC1
2	感染	OA-PC1	操作端末 1
3	感染	操作端末 1	コントローラ 1
4	不正通信	コントローラ 1	制御対象機器 1

4. 考察

今回，訓練シナリオ生成機における攻撃シナリオの生成に着目し検討を行った．その結果，訓練対象のサイバー攻撃事例が増加すればするほど訓練シナリオの再定義作業が増加するという課題に対し，訓練シナリオの再定義作業を効率化するための方法を提案した．本手法は，訓練したいサイバー攻撃事例を訓練対象のプラントのシステム構成で実行できるように内容を修正・補完するものである．これにより，教官の訓練シナリオ定義の作業コストが低減される．さらに，一度入力したシナリオとプラントのシステム構成を記憶しておくことで，新規のプラントに対するシナリオ定義や，新規のサイバー攻撃事例発生時のシナリオ定義作業において流用でき，この点においても作業コストを低減できた．

一方で，今回提案を行った方法は，訓練対象システム内での攻撃経路の一つを抽出し訓練シナリオに落とし込むというものである．しかし，現実のサイバー攻撃事例では，同一の攻撃事例であっても攻撃経路が単一であるとは限らない．そのため，上記のような現実を反映したシナリオ生成方法を検討する必要がある．

その他の残課題として，シナリオ作成の完全自動化があると考える．具体的には，今回の提案では基本攻撃シナリオの入力はあくまで人手で行っている点であり，シナリオ定義作業の省力化は行えても 0 にはなっていない．また，シナリオ定義を行う担当は，最新のサイバー攻撃事例を常にウォッチする必要があるため，その役割をプラント従事者が行う場合は専門領域が異なり負荷が高いと考えられる．

これらの課題に関しては，今後の検討で解決していきたい．

5. むすび

産業制御システム向けのサイバー攻撃事例の訓練シナリオの生成方法について提案を行った．従来方法では，複数の産業制御システムのプラントのシステム構成を反映したシナリオを生成するには，プラントのシステム構成毎に仮想環境を構築し，さらに新たなサイバー攻撃のシナリオを追加したい場合は，その都度シナリオを再定義する必要があり作業コストが増大する，という課題がある．

本課題を解決するために, 各プラントのシステム構成(機能及びネットワーク構成), と訓練させたいサイバー攻撃の必須ステップから，シナリオを実行するためのステップを生成する方法を提案した．今後は本方法に基づいた訓練シナリオ生成機を試作・評価していく．

謝辞 ．

本稿をまとめるにあたり，三菱電機の時田俊雄氏のご助力をいただきましたことに心より感謝申し上げます．

参考文献

[1] 日経 BP 社, “原子力発電所の設備を狙う「Stuxnet」” http://itpro.nikkeibp.co.jp/article/COLUMN/20120605/400482/?ST=attack&P=2, 2016 年 1 月 29 日確認
[2] IPA, “重要インフラの制御システムセキュリィと IT サービス継続に関する調査” , 2009 年 3 月
[3] 日本シーサート協議会, http://www.nca.gr.jp/2010/stuxnet/, 2016 年 1 月 29 日確認
[4] Nicolas Falliere, Liam O Murchu, and Eric Chien, "W32.Stuxnet Dossier Version 1.4", February 11, 2011
[5] 小熊 信孝, “Stuxnet －制御システムを狙った初のマルウエアー”, JPCERT/CC 2011 年 2 月
[6] P. García-Teodoro, J. Díaz-Verdejo, G. Maciá-Fernández and E. Vázquez, “Anomaly-based network intrusion detection: Techniques, systems and challenges”, Computers & Security, vol. 28, no. 1–2, pp. 18–28, 2009.
[7] 山口晃由, 中井綱人, 清水孝一, 小林信博, “プラント制御システムにおけるホワイトリスト型攻撃検知機能の可能性について”, SCIS 2016, 2016.
[8] 三菱電機,

ⓒ 2016 Information Processing Society of Japan

http://www.mitsubishielectric.co.jp/service/thermal/engineering_tool/index.html, 2016 年 1 月 29 日確認
[9] 株式会社オメガシミュレーション, http://www.omegasim.co.jp/solution/ots/, 2016 年 1 月 29 日確認
[10] McAfee, McAfee Labs 脅威レポート 2015 年 8 月(2015)
[11] Symantec, 2015 年インターネットセキュリティ脅威レポート (2015)
[12] 制御システムセキュリティセンター, 制御システムセキュリティセンター 東北多賀城（CSS-Base6）開所式 開所記念シンポジウム, 2013 年 5 月 28 日
[13] 小林 偉昭,“CSSC の進めるテストベッド CSS-Base6 と EDSA 認証について ～セキュアな制御システムを世界へ未来へ～”, 2014 年 2 月 5 日
[14] 木内 誠, “ICS のサイバーセキュリティへの取り組み 今、生産制御システム(ICS)が狙われている！”, 2015 年 4 月
[15] 宮内大, 益田修一郎, 鶴薫: 実環境を模擬したサイバー攻撃検知訓練環境, 電子情報通信学会総合大会講演論文集, 情報・システム 1, pp.104(2014)

ⓒ 2016 Information Processing Society of Japan