Computer Security Symposium 2017
23 - 25 October 2017

重要インフラ事業者における効果的なサイバー攻撃訓練に関する考察

宮地 美希[†1]　長谷川 弘幸[†1]　澤井 志彦[†1]
糠谷 友海[†2]　中田 圭亮[†2]　永野 憲次郎[†2]

概要：現状のサイバー攻撃発生を想定した訓練は，各社の CSIRT やセキュリティ担当者向けが大半であるが，現実のサイバー攻撃発生時は，CSIRT だけではなく経営層，危機管理担当者など種々の関係者，さらに，重要インフラ事業者では OT 系システム担当も含めた協働体制が必要である．サイバー攻撃訓練を効果的に実施するためには，全体をコーディネートした上で目的を絞った訓練を個々の関係者と実施する必要がある．その際，実際のサイバー攻撃対処の体制をインシデント対応のフローとして整理し，必要なスキル・見識を明確にし，その役割に沿った訓練内容にする．本稿では，我々の実施した各種訓練の実例をベースに，効果的なサイバー攻撃訓練を考察する．

キーワード：インシデント対応，重要インフラ事業者，訓練

A case study of effective cyberattack-exercises for leading infrastructure providers

Miki Miyachi[†1]　Hiroyuki Hasegawa[†1]　Yukihiko Sawai[†1]
Tomomi Nukaya[†2]　Keisuke Nakata[†2]　Kenjiro Nagano[†2]

Abstract: Current cyberattack-exercises are generally coordinated for CSIRT / cybersecurity section, but in reality cooperation with not only CSIRT but also executives, risk management department, public relations department and OT system department is needed in case of leading infrastructure providers. Due to a variety of sections concerned, it is important to manage overall cyberattack-exercises and implement limited ones for each section in order to make them efficient. To the more, after we prepare for a flowchart of incident-handling for cyberattack and clarify necessary skills and knowledge, we should arrange cyberattack-exercises aligned with each role .In this paper, we describe efficient cyberattack-exercises based on our cases of ones.

Keywords: Incident Handling, Leading Infrastructure Providers, Training

1. はじめに

サイバー攻撃がますます巧妙化するなか，各組織では侵入防護等のセキュリティ対策を強化するだけではなく，セキュリティインシデントが発生した際にいかに対処するかが重要となっている．

各組織で一般に SOC（Security Operation Center）や CSIRT（Computer Security Incident Response Team）と呼ばれる体制の整備が進んでいる．SOC は，セキュリティインシデントを検知した際に初動対応を行う体制の総称で，監視・検知箇所にもよるが一般的に外部サービスにより整備しているケースが多い．CSIRT は，コンピュータセキュリティにかかるインシデントに対処するための体制の総称で，インシデント関連情報，脆弱性情報，攻撃予兆情報を常に収集，分析し，対応方針や手順の策定などの任務を担うのが一般的である[1].

CSIRT の任務は，サイバー攻撃の巧妙化に伴い，高度化・多様化している[2]．さらに，重大なセキュリティインシデントが発生した際は，組織内外の様々な関係者・専門家と協働して対処することになる．このため，セキュリティインシデント発生時の CSRIT の役割は非常に重要であり，対処能力向上のためにサイバー攻撃訓練が必須である．

そこで，本稿では，実際のサイバー攻撃への対処に対する現状の課題を整理する．その上で，我々の実施した各種訓練の実施内容・目的およびその結果を考察し，効果的なサイバー攻撃訓練を提起する．

2. サイバー攻撃訓練の事例

組織内のサイバー攻撃訓練のほか，多数の組織が集まり，合同でサイバー攻撃訓練を実施する事例が国内外で見受けられる．

米国では，北米電力信頼性評議会（NERC : North American Electric Reliability Corporation）が中心となり，政府関係者

†1 中部電力株式会社
CHUBU Electric Power Co., Inc.
http://www.chuden.co.jp/index.html

†2 株式会社中電シーティーアイ
ChudenCTI Co., Ltd.
http://www.cti.co.jp/

や電力事業者を集めて GridEx（Grid Security Exercise）と呼ばれる訓練を，2011 年より隔年で実施している．2015 年 11 月に第 3 回が実施され，カナダ，メキシコといった米国外の事業者も含め、350 以上の組織が参加し、インシデントレスポンスや情報共有についての演習に加え，Executive Tabletop と呼ばれる上級マネージャークラスによるディスカッションが実施された．Executive Tabletop のディスカッションでは，物理攻撃やサイバー攻撃により大規模停電が発生した場合の対応施策，意思決定内容などが議論された[3].

日本では，内閣サイバーセキュリティセンターが，重要インフラ事業者や政府機関等を集めて分野横断的演習を主催している．至近では，2016 年 12 月 7 日に第 11 回目が開催され，重要インフラ事業者 44 機関を含む 505 組織，約 2,080 名が参加した[4].

さらに，各都道府県警察は各地の重要インフラ事業者等と合同で訓練を実施する取り組みを進めている．

警視庁は，2020 年東京オリンピック・パラリンピックを見据え，電力，ガス，鉄道などのインフラ事業者とのサイバー防衛訓練を実施するなど，官民連携を強化している[5]. 愛知県警察は，サイバーテロ想定緊急対処共同訓練を実施，事前にシナリオ等の想定を被訓練者に知らせないブラインド型で訓練遂行することで事案対処能力の向上を図っている[6].

3. 課題提起

3.1 重大なサイバー攻撃事案への対処

サイバー攻撃を想定した訓練は各箇所で実施され，CSIRT の対処能力は確実に向上していると評価される．

しかし，重大なサイバー攻撃事案が発生した場合は，CSIRT だけでなく，組織内の様々なセクション・階層が関係する．

経営に直結する重要な判断・意思決定を行う経営層をはじめ，サイバー事案も含めた組織全体の危機管理を担う危機管理担当，プレス発表等対外発信を担う広報担当なども重要な役割を担う．

セキュリティ関連は専門性が高いこともあり，サイバー攻撃への対処は「CSIRT が考えればいい!!」と思われることもある．CSIRT に対する期待は大きいものの，現実のサイバー攻撃対処は CSIRT のみでは不十分である．

3.2 重要インフラ事業者の実情

重要インフラ事業者では，システムのなかに，事務処理系システムとも呼ばれる IT（Information Technology）系システムに加え，制御系システムとも呼ばれる OT（Operational Technology）系システムが存在する．

OT 系システムは，従前は独自プロトコル・仕様が使用されていることからサイバー攻撃を受けるリスクは低いと考えられていた．しかし，近年 OT 系システムに汎用技術が使用されるようになったことに加え，ネットワークに接続されるケースが増加し，サイバー攻撃を受けるリスクが高まっている．

さらに，OT 系システムは多種多様であり，かつ OT 系システムに関する装置類は一部集約化が進んでいる事例があるものの，物理的に分散配置されている場合が多いという特徴がある．このため，IT 系システム担当が，組織内のすべての OT 系システム詳細を把握することが困難であり，OT 系システムへのサイバー攻撃が想定される場合の対処方法を確立する必要がある．

一般的に，CSIRT は IT 系システムをバックグラウンドに持つ要員で構成されることが多い.「CSIRT」の定義にもよるが，OT 系システム担当は CSIRT の一員となるよりもサイバー攻撃事案発生時は CSIRT と連携して対処にあたることが多い.

3.3 課題提起まとめ

実際のサイバー攻撃への対処は，特に重大事案となった場合は経営層を含めて組織内の様々な関係箇所が協働する必要がある．

また，重要インフラ事業者では多種多様な OT 系システムを保有している．サイバー攻撃が OT 系システムに及ぶ場合，OT 系システム担当と協働したインシデント対応が重要である．

サイバー攻撃への対処に関する関係者をまとめると，表 1 のとおりとなる．

表 1　関係者一覧

Table 1　List of Roles for Cyber Incident Handling

関係者名称	役割
経営層	経営に直結する重要な意思決定
CSIRT	セキュリティインシデントの事象把握，対応状況把握，対処の総指揮
SOC	セキュリティインシデントの監視・初動対応
IT 系システム担当	IT 系システムの管理・把握
OT 系システム担当	OT 系システムの管理・把握
広報担当	プレス等の対外発信
危機管理担当	組織全体の危機管理総括

さらに，サイバー攻撃事案は自然災害と比較して状況や様相が掴みにくい．通常業務でサイバー攻撃事案と触れることのない関係者は，訓練によってサイバー攻撃事案に関するイメージを醸成しておくことが必要である．

したがって，サイバー攻撃訓練は，CSIRT のサイバー攻撃対処能力向上だけでなく，以下の目的を企図して実施する必要がある．

- 多種多様な関係者が協働できるようにする

- システム担当ではない関係者に対するサイバー攻撃事案のイメージ醸成・理解

4. 各種訓練の概要

我々は, 表 2 に示す様々なサイバー攻撃訓練を実施した.

表 2　サイバー攻撃訓練一覧

Table 2　List of Cyberattack-exercises

訓練名称	訓練参加者
経営層訓練	経営層，CSIRT
IT 系システム実機訓練	IT 系システム担当，CSIRT
OT 系システム侵入を想定した対処訓練	OT 系システム担当, IT 系システム担当，CSIRT
SOC との情報伝達訓練	SOC 運用者，CSIRT
危機管理担当との情報伝達訓練	危機管理担当，CSIRT

以下に，各訓練の実施内容等の詳細を述べる.

4.1 経営層訓練

(1) 実施内容・目的

重大なサイバー攻撃事案が発生した際，被害拡大防止策を迅速に実行に移すのが重要であり，迅速な対処が企業ブランドにも直結する.

しかし，被害拡大防止策は，業務影響・お客さま影響のあるものが通常であり，CSIRT の判断ではなく，経営層による経営判断が重要となる.

経営層訓練では，想定シナリオに基づき，サイバー攻撃に関する状況説明および取るべき選択肢を説明した後，訓練者である経営層でディスカッション，最終的に意思決定を行うことを実施した.

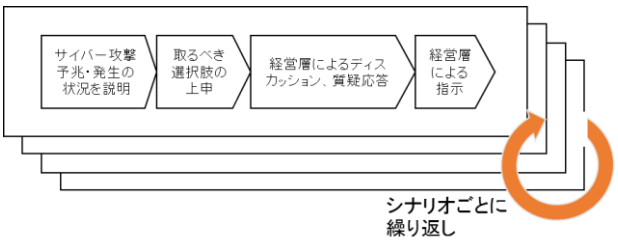

図 2　経営層訓練の進め方

Figure 2　Flow of Executive-Training

訓練の主目的は以下の通りである.

- サイバー攻撃特有の影響が不明確な状態での経営層との意思疎通確認
- サイバー攻撃発生時の意思決定プロセス

訓練の内容・進め方に関し，特に留意した点は，経営層に対して意思決定を求める場面を想定し，その状況に近いシナリオを用意することである.

一般にサイバー攻撃事案が発生した場合，内容が専門的であることから CSIRT に対応を委ねられていることも多い．そういった状況で，CSIRT から経営層に対して意思決定を求めても「任せた！（Do IT!）」と回答するよりないのであれば，訓練の意味はない.

本訓練では，状況説明として，サイバー攻撃特有の不明確な状況，事象があいまいな状況を用意し，提示する選択肢として，どの選択肢を選んでも業務影響・お客さま影響など会社として何等か損害を受けるものを用意することとした.

状況説明は，例えば以下のような内容とした.

- 攻撃者がインターネット上で当社に対してサイバー攻撃の犯行予告を行ったが，実際の攻撃は確認できていない.
- 制御系システムを狙ったサイバー攻撃の痕跡は見つかったが，新種の攻撃のため当社サービスや業務等への影響は不明である.

状況説明後，取りうる選択肢を 2〜3 つ説明し，その内容について経営層でディスカッションを行い，最終的に何らかの意思決定を出すということを繰り返した.

(2) 実施結果

経営層訓練は，訓練事務局が構想した想定シナリオに合致した意思決定結果に到達することが目的ではない．あいまい模糊とした状況下で, 今後何が起こりうるかを想像し，短い時間で何らかの意思決定･結論に導くのが目的である.

経営層訓練を通して，サイバー事案の特徴について経営層の理解が深まったことが最大の成果であった．また，CSIRT にとっても，経営層とコミュニケーションする貴重な機会となった.

なお，訓練事務局は訓練準備として想定シナリオや取るべき選択肢を用意するが，IT 系システム，OT 系システムの実態を把握したうえで検討することが必要であるため，結果として，訓練事務局のスキル向上にも寄与した.

4.2 IT 系システム実機訓練

(1) 実施内容・目的

事業者として一番の脅威は標的型攻撃である．不特定多数を狙ったサイバー攻撃は，一般的なセキュリティ製品で検知・防御が可能なことが多いが，標的型攻撃ではパターンマッチング型の技術では検知が困難である.

IT 系システム実機訓練では，実機・本番環境において，IT 系の端末がマルウェア感染した状況を想定し，その後のマルウェアの活動をいかに検知するかの検証を実施した.

実機・本番環境での訓練実施は，業務影響が懸念されるが，IT 系システム担当者と綿密に事前調整し，訓練当日も

IT 系システム担当者が参画することで，システム停止等の業務影響リスクに対処した．

(2) **実施結果**

IT 系システムには，IPS 等のセキュリティ製品以外に，各種 NW 機器やサーバがあり，ログを保持している．これらは，元々セキュリティ対策のために設計して取得しているわけではないが，なかにはマルウェア検知に有用なログも存在する．

実機・本番環境で当該訓練を実施することによって，IT 系システムの各種ログからいかにマルウェアの挙動を検知できるかの知見を得ることができる．

4.3 OT 系システム侵入を想定した対処訓練

(1) **実施内容・目的**

「平成 25 年度次世代電力システムに関する電力保安調査報告書」[7]でも述べられているように，IT 系システムと OT 系システムがデータ連係等接続する例が増えている．

サイバー攻撃は様々な目的が想定されるが，近年では OT 系システムの停止を狙った攻撃が社会問題となっている．重要インフラ事業者は IT 系システムへのサイバー攻撃に加え，OT 系システムへのサイバー攻撃を想定脅威とする必要がある．

OT 系システムへのサイバー攻撃は，様々な侵入ルートが考えられるが，なかでも IT 系システムを経由して OT 系システムへ侵入するルートは，種々のシステムを経由することから，関係者が多数となり情報収集や影響把握が困難な場合がある．

本訓練では，IT 系システムから OT 系システムへの侵入を想定し，IT 系システムがサイバー攻撃を受けた前提で，OT 系システムへ波及していくシナリオについてインシデントハンドリングの訓練を実施した．

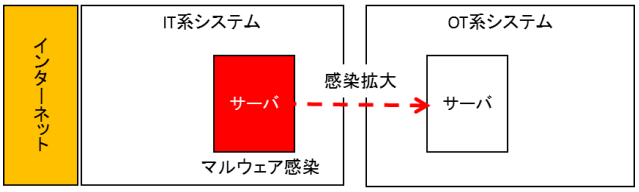

図 3　訓練シナリオイメージ

Figure 3　Image of Training Scenario

(2) **実施結果**

OT 系システム担当者は，通常業務でサイバー攻撃手法やマルウェア感染ルート・手法に触れる機会が少ないケースがある．訓練を通じて，OT 系システム担当者にセキュリティに関する意識向上につながった．

また，IT 系システムと OT 系システムが接続に関し、それぞれの担当者がマルウェア感染拡大等のリスクをディスカッションすることで，システム仕様等の相互理解が深まることにもつながった．

4.4 SOC との情報伝達訓練

(1) **実施内容・目的**

SOC は，セキュリティインシデントの監視から初動対応を行い，必要に応じて CSIRT にエスカレーションする機能を持つ．

CSIRT および SOC を同一組織内に体制構築している例もあるが，SOC を外部委託し，CSIRT 機能を内製化していることが多い．我々においては，CSIRT は中部電力および中電シーティーアイの混成体制，SOC は中電シーティーアイが担務している体制である．

サイバー攻撃事案が発生した場合，CSIRT はインシデントハンドリングのため，様々なログの調査，フォレンジクスなどを実施する必要があるため，現実には CSIRT にエスカレーションした後も，SOC と CSIRT は一体となってハンドリングを行う必要がある．

重大なサイバー攻撃事案が発生すると，影響範囲は多岐にわたることも想定され，CSIRT と SOC の情報連絡は非常に密になることが想定される．その際，情報が錯そうする状況も想定されるため，あらかじめ訓練により，CSIRT から SOC への指示が迅速かつ正確に伝わるかを目的として訓練を行った．

(2) **実施結果**

SOC と CSIRT は，日常業務において密に連携していることから，基本的な用語等に関して認識の齟齬等の混乱は生じず，スムーズに情報伝達ができた．

しかし，重大なサイバー攻撃事案発生を想定して，様々なインシデントが同時発生，ステータスが時々刻々と変化する状況としたので，情報の錯綜・混乱が発生した．

サイバー攻撃への対処では，状況の把握および関係箇所への確実な報告が CSIRT の重要な役割であるため，SOC と CSIRT で錯綜すると適切な対処ができない．

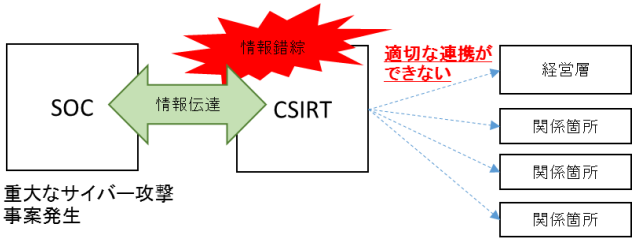

図 4　SOC との情報伝達訓練の意義

Figure 4　Object of Information-Sharing-Training Cooperated with SOC

たとえ日常業務で SOC と CSIRT とが連携していたとしても，日常業務にない重大なサイバー攻撃事案が発生した場合は，日常業務と同様に情報伝達ができるとは限らない．

したがって，訓練を実施して経験を積むことが重要であり，また，情報伝達の効率化のためのツールを準備しておくことも有効であると言える．

4.5 危機管理担当との情報伝達訓練

(1) 実施内容・目的

サイバー攻撃により会社に重大な影響を及ぼすことが想定される場合，危機管理担当が状況把握，対応体制構築などの任務を担う．

危機管理担当は一般に IT の専門家ではないため，CSIRT からサイバー攻撃事象等の情報に関する説明を受けた際に，サイバー事象ひいては用語を理解するため，訓練を受けておく必要がある．

(2) 実施結果

訓練目的のとおり，サイバー事案に関する危機管理担当者の理解について，訓練を通じて深めることができた．

今後，サイバー事案とその他の事案が複合的に発生する状況も想定されること，自然災害等発生時の混乱に乗じてサイバー攻撃が行われることも想定されるため，このように危機管理担当がサイバー事案に関する理解を深めることは有意義である．

5. 考察

これまで，様々な観点・参加者によるサイバー攻撃訓練の実施内容を述べてきた．

「3.課題提起」で論述したように，特に重要インフラ事業者においては，セキュリティインシデント発生時は様々な立場・役割が関係するので，それぞれが有機的に協働し機能させることが重要であり，そのために効果的なサイバー攻撃訓練を実施する必要がある．

(1) サイバー攻撃事案の特殊性

何等か訓練を行う際，すべての関係者を一堂に介して実施することが通常である．

我々においても，大規模地震等の自然災害が発生した場合を想定した防災訓練では，全社的な体制にて対処するため，関係箇所すべてが訓練に参加して，指揮命令系統の確認，情報伝達・収集等の手順確認などを目的として実施している．

しかし，サイバー攻撃に関する訓練は，自然災害発生時の訓練と様相が異なる．

自然災害の場合，設備損壊など何らかの明確な災害が発生した時点をスタートして，被害状況の情報収集や復旧，関係機関等への報告など，関係箇所が一斉に各々の役割に則った対処を行うことになる．

サイバー攻撃事案の場合，明確な被害発生が訓練のスタートとなるわけではなく，何らかのセキュリティインシデントが発生し，各種調査等を行い，その結果，IT 系システム担当者，OT 系システム担当者への波及，さらに具体的な被害が発生しうる，あるいは発生した場合にシナリオが進展し，経営層の意思決定，危機管理担当や広報担当等の関係者との調整など，対処等すべき関係者が広がっていく．

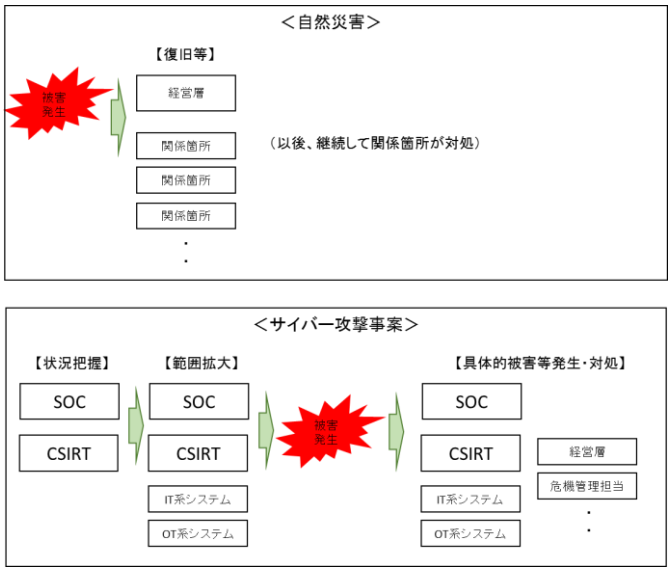

図 5　自然災害とサイバー攻撃事案の違い

Figure 5　Image of Differences Between Natural Disaster and Cyberattacks

(2) サイバー攻撃訓練中の稼働状況

サイバー攻撃訓練を行う際，すべての関係者を一堂に介して訓練を行うと，個々の関係者は，訓練シナリオの一場面でその役割を求められるため，待ち時間が多く非効率と考えられる．

「4.各種訓練の概要」に記載した我々の各訓練の参加人数および訓練時間は，表 3 のとおりである．

表 3　サイバー攻撃訓練時間

Table 3　Time for Cyberattack-exercises executed

訓練名称	訓練参加人数	訓練時間
経営層訓練	経営層：10 人	1.5 時間
IT 系システム実機訓練	IT 系システム：8 人	4 日間
OT 系システム侵入を想定した対処訓練	OT 系システム担当：21 人 IT 系システム担当：8 人 CSIRT：3 人	2 時間
SOC との情報伝達訓練	SOC：5 人 CSIRT：6 人	2 時間
危機管理担当との情報伝達訓練	危機管理担当：2 人 CSIRT：2 人	2 時間

仮に，図 4 に示したサイバー攻撃事案の場合の，「状況把

握」,「範囲拡大」,「具体的被害等発生・対処」の各フェーズが均等に訓練時間を割り当てられたとした場合，時間換算で約 1/3 が訓練時間中その役割がなく待機状態で過ごす計算となる．

(3) 効果的なサイバー攻撃訓練

関係者を一堂に介した訓練では，上述のように待ち状態の訓練参加者が存在するためことから，効果的・効率的なサイバー攻撃訓練とするには，目的を絞った訓練を個々の関係者と実施する必要がある．

その場合，CSIRT がサイバー攻撃対処の中核を担う前提で，CSIRT が実際のサイバー攻撃対処体制の全体像を把握し，個々の訓練をコーディネートしなければならない．

実践的には，セキュリティインシデント発生からサイバー攻撃への対処に関するフェーズおよびフローを整理し，関係箇所の役割を明確にし，関係箇所のスキル・見識の実態に沿った訓練内容にする．

図 6 に,「サイバー攻撃発生時の対処フロー」の例，表 4 に,「状況把握」,「範囲拡大」,「具体的被害等発生・対処」の 3 つに分けた場合の、各フェーズにおけるサイバー攻撃対処の課題の例を示す．

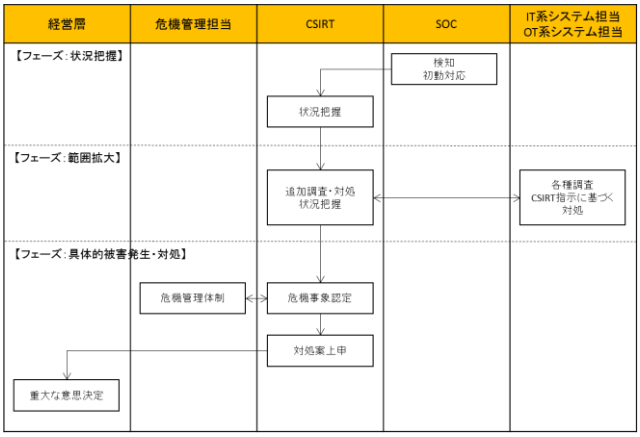

図 6　サイバー攻撃発生時の対処フロー例

Figure 6　Example of Flowchart of Cyberattack-Handling

表 4　フェーズ毎の課題例

Table 4　Example of Issues for Cyberattack-Handling

フェーズ	サイバー攻撃対処の課題例
状況把握	・重大なサイバー攻撃事案発生時の CSIRT-SOC の情報共有
範囲拡大	・CSIRT のインシデントハンドリング能力 ・OT 系システム担当との連携
具体的被害等発生・対処	・経営層とのコミュニケーション ・危機管理担当とのコミュニケーション

このようにフェーズを分けることで，訓練対象者を限定した効率的なサイバー攻撃訓練を企画することができる．

また課題が明確になれば，その課題に沿う訓練内容，訓練参加者，訓練シナリオを企画し，画一的な訓練内容・シナリオするよりも効果的なサイバー攻撃訓練を実施することができる．

6. おわりに

本稿では，サイバー攻撃訓練を効果的に実践する方法について，我々で実施した各種訓練の実例をベースに考察した．

サイバー攻撃はますます巧妙化し，サイバー攻撃を 100%完全に防護することは不可能であるため，サイバー攻撃発生時のインシデント対処能力を向上することが，組織のリスク管理上重要なテーマとなっている．

インシデント対応といった危機管理能力は，最終的には“人”に依存するため，個々のスキル・能力の向上を地道に進めることが重要である．訓練に時間を割くのが難しいのが多くの実情であろうが，限られた時間のなかで効果的・効率的に訓練を行うために，本稿の内容が役に立てば幸いである．

重要インフラ事業者は，地域社会に直結したサービスを提供している．サイバー攻撃によってインフラサービスが停止するリスクが看過できない状況となった今，重要インフラ事業者間や地域社会が連携して対処することも重要であると考えている．

今後，今まで以上に産官学連携を進め，地域全体でサイバー攻撃に対処する機運を高めていきたい．

謝辞　本稿では，サイバー攻撃訓練の実施および執筆にあたり，社内外の関係者に協力を仰ぎました．ここに深く感謝申し上げます．

参考文献

[1]　日本シーサート協議会　シーサートとは？ http://www.nca.gr.jp/outline/index.html.
[2]　日本シーサート協議会　CSIRT 人材の定義と確保 ver1.5 . http://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf, (参照 6 頁)
[3]　Grid Security Exercise GridExⅢReport
[4]　NISC 2016 年度「分野横断的演習」について https://www.nisc.go.jp/conference/cs/ciip/dai10/pdf/10shiryou05.pdf, (参照 2 頁)
[5]　日本経済新聞記事 「警視庁，インフラ事業者とサイバー防衛訓練」 http://www.nikkei.com/article/DGXLASDG24H0X_U7A120C1CC0000/
[6]　愛知県警察本部　サイバーテロ対策　「サイバーテロ想定緊急対処共同訓練の実施」 https://www.pref.aichi.jp/police/anzen/kouan1/cyberterro.html.
[7]　経済産業省ホームページ　平成 25 年度次世代電力システムに関する電力保安調査報告書 http://www.meti.go.jp/meti_lib/report/2014fy/E003791.pdf(参照 59 頁).