インシデント発生時における組織間コミュニケーション訓練の設計と評価

山内 正人[1] 岡田 光代[1] 加藤 大弥[1] 坂倉 基司[2] 半澤 恒[3] 砂原 秀樹[1]

概要：本稿ではサイバーセキュリティインシデント発生時における組織間コミュニケーション訓練のための演習設計とその評価について述べる。サイバーセキュリティインシデントの増加に伴い組織においてサイバーセキュリティインシデントが発生した場合に備えた対応手順などの策定が進んでいる。また、実際に発生した場合に備えて研修や対応訓練などが行われている。特にサイバーセキュリティインシデントは組織内における特定の専門家のみが対応出来れば良いものではなく、物理的に離れた場所に居る人も含め様々なロールの人が連携して迅速に対応する必要がある。そこで本研究では物理的に離れた場所にある組織間のコミュニケーションも考慮したサイバーセキュリティインシデント対応演習を設計し、実際にその様な状況での対応も想定される企業で実施した結果について述べる。実施した結果、繰り返し訓練することで対応にかかる時間短縮や対応手順の洗練などを確認出来たほか、参加者から演習が実践的な演習となっていたこともアンケート結果から確認した。

Design for security incident handling exercise considering interorganizational communication

Masato Yamanouchi[1] Miyo Okada[1] Daiya Kato[1] Motoshi Sakakura[2] Hisashi Hanzawa[3] Hideki Sunahara[1]

1. はじめに

本稿ではサイバーセキュリティインシデント発生時における組織間コミュニケーション訓練のための演習設計とその評価について述べる。サイバーセキュリティインシデントの増加に伴い組織においてサイバーセキュリティインシデントが発生した場合に備えた対応手順などの策定が進んでいる。また、実際に発生した場合に備えて研修や対応訓練などが行われている。特にサイバーセキュリティインシデントは組織内における特定の専門家のみが対応出来れば良いものではなく、物理的に離れた場所に居る人も含め様々なロールの人が連携して迅速に対応する必要がある。そのためには各組織に合致した状況で繰り返し組織間を跨ぐコミュニケーションの訓練が重要となる。これまでも多くのサイバーセキュリティインシデント対応訓練が開発されているが、その多くは専用の設備を必要としたり、準備コストが高く、容易に実施することが困難である。近年繰り返し容易に実施可能なゲーム形式の訓練も登場してきているがその多くは一同に会して実施するものが多く、組織間コミュニケーションの訓練となるものは少ない。そこで本研究では物理的に離れた場所にある組織間のコミュニケーションも考慮したサイバーセキュリティインシデント対応演習を設計し、実際にその様な状況での対応も想定される株式会社日立製作所で実施した。実施した結果、繰り返し訓練することで対応にかかる時間短縮や対応手順の洗練などを確認出来たほか、参加者から演習が実践的な演習となっていたこともアンケート結果からわかった。

1 慶應義塾大学大学院メディアデザイン研究科
2 株式会社 日立製作所
3 株式会社 日立インフォメーションアカデミー

2. サイバーセキュリティインシデント発生時における対応

サイバーセキュリティインシデント発生時における対応の基本的な流れを図 1 に示す。サイバーセキュリティインシデントの対応には事前準備から再発防止策の実施までが含まれる。

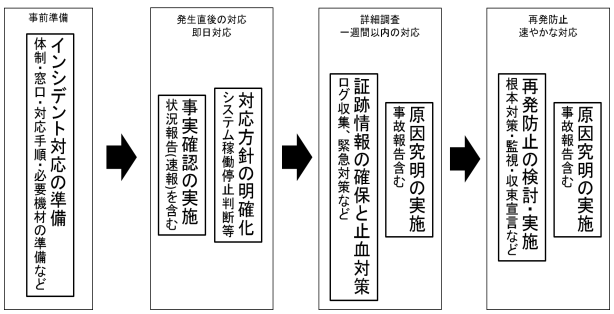


図 1 セキュリティインシデント対応の基本的な流れ

サイバーセキュリティインシデントが発生した際に備えて事前に対応手順の整備や、緊急時の体制、緊急時の連絡窓口、対応に必要となる機材準備、またそれらの周知等を行う。これによりサイバーセキュリティインシデントが発生した際に関係者は速やかに対応行動が出来る。

サイバーセキュリティインシデントが発生した直後は関係各所と連携し事実確認・状況把握を行い、確認した状況にあわせて事前に策定した手順に従って対応を行う。またシステムを継続稼働させながら対応を行うか稼働停止した上で対応を行うか等について状況やリスク、経済的損失等を総合的に考慮して判断を行う。

サイバーセキュリティインシデントに対する初動対応が終わると、証跡情報の確保や原因究明を行う。また対応手順の見直しや判明した原因から根本対策など再発防止の検討と実施を行い次回に備えた対策をする流れとなる。

これらの対応は組織の規模や組織構成により物理的に離れた場所にある部署間や組織間において連携の必要もあり、組織全体での事前対策や事前訓練が重要となる。

3. サイバーセキュリティ演習

事前訓練を行うための一つの有効な手段としてサイバーセキュリティ演習がある。サイバーセキュリティ演習は大きく分けると 2 種類あり、個別スキル演習と複合型演習がある。複合型演習はさらにシナリオ型演習とゲーム型演習に分けられる。図 2 に既存演習の対象範囲と本稿で述べる演習の対象について示す。

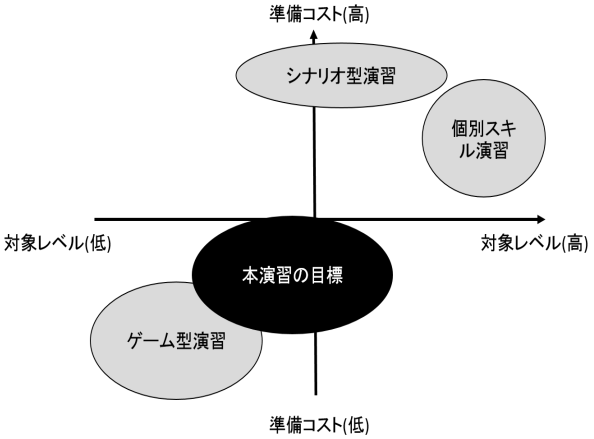


図 2 本演習の位置付け

3.1 個別スキル演習

個別スキル演習は静的解析や動的解析などの個々の解析スキルや攻撃に対する防御スキルなどを集中的に実施しスキルアップを目的とする演習である。主にエンジニアを対象とした上級者向けの演習が多い。参加するためにはエンジニアとして必要となる情報技術に関する前提知識が求められるとともに、エンジニアではない職種に対しての効果は限定的である。例えばセキュリティ教育プログラム SecCap[1] で実施されているシステム攻撃・防御演習 [2] では参加者は閉じられた環境内において脆弱性があらかじめ用意されたマシンに対して攻撃者視点での攻撃を実施し、それに対する防御の実施や防御方法の考察を行う。攻撃者視点での攻撃の実施には UNIX の知識やネットワークの知識、コンピュータの Character User Interface での操作、プログラミング等の知識が必要となる。防御の実施や防御方法の考察においても同様のスキル及びアセンブリ言語等の知識が必要となる。当該演習で得られた知識はシステムエンジニアがシステムを設計・運用する際やネットワークエンジニアが社内ネットワークを運用する際に重要となる一方それ以外の職種への効果は限定である。また個々のスキル向上には効果的であるが、実際の攻撃への対処は様々なスキルを駆使して対応が必要となるため単一のスキルだけでは対応が難しい場合もある。

3.2 複合型演習

複合型演習は、より実際の攻撃を意識して複合的にスキルを駆使してインシデントへ対応する能力を培う演習である。複合型演習は大きく分けるとシナリオ型演習とゲーム型演習に分類できる。

3.2.1 シナリオ型演習

シナリオ型演習はあらかじめ演習運営者が設定したシナリオに沿って演習が進行し、参加者は進行に沿って適切な対応を訓練する演習である。シナリオ型演習の一般的なシナリオの流れを図 3 に示す。

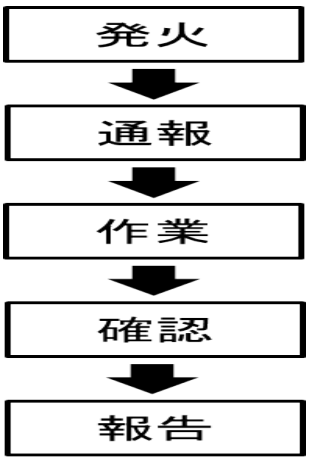


図 3 一般的なシナリオの流れ

シナリオの攻撃スクリプトが開始する発火フェーズから始まり、攻撃を察知し参加者に通報するフェーズ (演習によっては参加者が検知する場合もある) 、通報内容に基づいて適切な対処を行う作業フェーズ、作業が完了し問題が解決していることを確認する確認フェーズ、通報者等に対

して報告を行う報告フェーズまでを行う。例えばサイバー犯罪に関する白浜シンポジウムに併設して実施されている情報危機管理コンテスト [3] では参加者にサーバと電話機とパソコンが与えられる。コンテスト開始とともに攻撃者役の運営者が各参加者のサーバに対して攻撃を実施する。その後通報者役の運営者より各参加者に対して「自分の個人情報がネット上の掲示板に載っている」等の通報を行う。参加者はその通報に基づいて事実確認等の作業を行うが、その際に通報者に確認したい事が発生した場合は一般の人である通報者に対して電話でわかりやすく説明した上で確認する必要がある。そのため技術スキルとともにコミュニケーションスキルも求められる演習となっている。また対応作業を行う際に上長の許可が必要となる作業もあるため組織のガバナンスへの意識や通報者以外の顧客へのアナウンスなど様々なスキルを用いてインシデントへの対応を行うことになる。そのためより実践的な内容であったり、複数のスキルが向上できるメリットがある。一方でシナリオ型演習はシナリオ通り動作するシステム、環境を準備する必要があり準備コストが高い。図 4 に情報危機管理コンテストにおける和歌山大学の運営準備の様子を示す。図 4 では参加者が使用するサーバの設定やネットワークの設定、また通報者の台詞や参加者に対する返答の統一などの確認を行っている。またシナリオを一度実施すると 2 回目以降はどのような事が起こるのかわかってしまうため、反復して実施することが難しい。

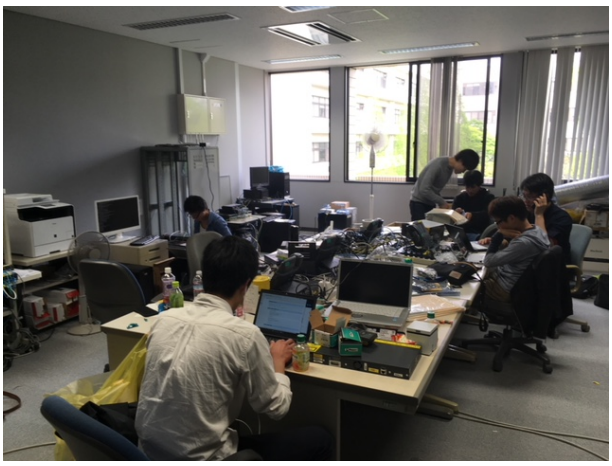


図 4 情報危機管理コンテストの運営準備の様子

以下にシナリオ型演習のメリットとデメリットについてまとめる。

- メリット
  - 実例に基づいた忠実なシナリオが作成可能
  - 解析技術等の複数スキルの向上
- デメリット
  - 準備コストが高い
  - 参加者に解析技術等のスキルが求められる
  - シナリオが同じため反復して実施するのが難しい

3.2.2 ゲーム型演習

ゲーム型演習はボードゲームやカードゲーム等のゲーム形式でセキュリティインシデントを体験して対応する訓練を行う演習である。ゲーム型演習はセキュリティベンダー各社がボードゲーム型やカードゲーム型などの演習教材を開発している [4], [5], [6]。シナリオ型演習に比べて準備コストが低く、またゲームの進行が毎回変化するため反復して実施出来ることが特徴である。また、実際に解析を行う等の作業も少ないため、前提となる要求スキルが低く様々な人が参加しやすいのも特徴である。

以下にゲーム型演習のメリットとデメリットについてまとめる。

- メリット
  - 準備コストが低い
  - 反復して実施可能
  - 要求スキルが低い
- デメリット
  - スムーズな進行はファシリテータのスキルに依存
  - 細部の設定が曖昧な場合が多い

その多くは一同に会して実施するものが多く、組織間コミュニケーションの訓練となるものは少ない。

3.3 本研究の目的

前節までで述べてきた既存の演習をまとめると前提となる知識・スキルが低く幅広い職種へ効果が期待できるゲーム型演習やセキュリティのわかるエンジニアを育成するためのシナリオ型演習や個別スキル演習は存在するもののその多くは一同に会して実施するものが多く、組織間コミュニケーションの訓練となるものは少ない。特にインシデント発生時は物理的に離れた場所にいることも想定される関係者間のコミュニケーションが重要となるがその様なコミュニケーションの訓練を主眼とした演習は少ない。またインシデント発生時におけるコミュニケーションは幅広い職種に求められるスキルであり、組織内に浸透させるためには何度も繰り返し実施する必要があり、準備コストが低く反復実施可能であることも重要な要素である。そこで本研究では既存のゲーム型演習を応用することで準備コストが低く反復して実施可能なコミュニケーション訓練の演習を開発することを目的とする。

4. 組織間コミュニケーション訓練

演習は 2 つのグループとファシリテータによって行われる。それぞれのグループが本社組織やデータセンタ組織等異なる組織と設定する。演習の流れ及びグループの構成を図 5 に示す。図 5 に示した通り、各グループ (組織) はそれぞれ違うイベントが通知されるため、各グループ (組織) に設置されたコミュニケーションチャネルを使用してイベン

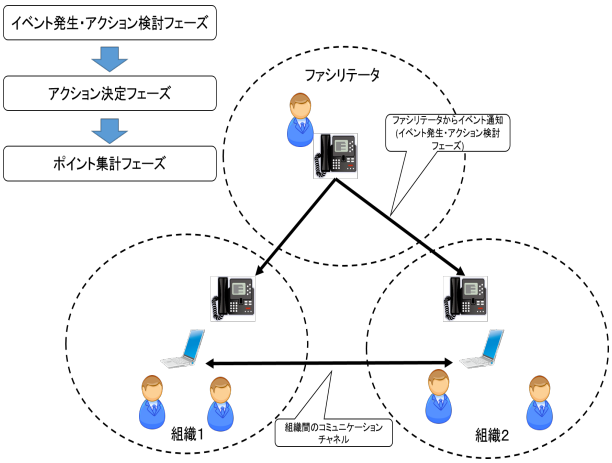


図 5　演習の流れ及びグループの構成

トや状況の共有及びそれに基づいた対応について迅速に連携しながら決定する。

5.　演習の流れ

演習の流れは下記の通りである。

(1) イベント発生・アクション検討フェーズ
(2) アクション決定フェーズ
(3) フィードバックフェーズ

5.1　イベント発生・アクション検討フェーズ

本フェーズではイベントが発生したことを知らせるため、ファシリテータから組織 1 及び組織 2 に対して異なる内容のイベントが通知される。例えば外部からの問い合わせは組織 1 へ、組織 2 に所属する社員からの報告は組織 2 へ通知される。その後各組織に所属するプレイヤーは制限時間内に組織内及び組織間で連携しアクションを決定する。制限時間はプレイヤーが初めての場合は 20 分程度、1 度でもプレイしたことがあるプレイヤーの場合は 15 分程度に設定した。イベントに対して各組織で取り得る対応が書かれたアクションカードを用意しておく。組織 1 及び組織 2 にそれぞれ異なるアクションカードを用意しておき、組織 1 と組織 2 併せて 2 枚のアクションカードを決定する。

5.2　アクション決定フェーズ

アクション決定フェーズは最終意思決定の役割をもった組織側よりファシリテータへ決定したアクションを連絡する。アクション検討フェーズで 2 枚のアクションカードが決まらなかった場合は最終意思決定の役割を持った組織が最終決定を行い連絡する。

5.3　フィードバックフェーズ

ファシリテータが対応時のコミュニケーション状況を確認し、ゲーム終了後にフィードバックを行う。事前にコミュニケーションの基礎的なポイントを決めておき、ファシリテータはその項目にしたがってプレイヤーが出来ているか確認する。下記にコミュニケーションの基礎的な確認事項の例を示す。

- 報告
  - インシデント通知後 3 分以内に相手組織に報告をした
  - 事実を 5W1H で簡潔に伝えた
  - 事実をより理解するための背景を 5W1H で簡潔に伝えた
- コミュニケーション
  - 相手組織からの連絡に都度対応した
  - 相手組織の状況と背景の理解に必要な情報を相手組織から得られた。また必要があれば相手組織へ質問した。
  - 導入・挨拶・敬語など、相互関係が円滑に進む言葉が付いている

また組織 1 と組織 2 間の双方向コミュニケーションチャネルをチャット等のテキストベースのコミュニケーションツールとしておくことでファシリテータがフィードバックを行う際に確認しやすく、プレイヤーも事後に振り返りを行うことが出来る。

6.　演習の実施

6.1　演習環境

日立製作所社内からの公募により 17 名の参加者があり、3 グループでの実施とした。各グループは図 5 で示した構成とし、各グループの内訳はファシリテータ 1 名、各組織にそれぞれ参加者 3 名とした。組織はサービス運営組織 (決定権あり) とデータセンターとし、サービス運営組織用、データセンター用、ファシリテータ用の 3 部屋用意することでファシリテータ及び各組織が直接コミュニケーション出来ないようにした。また各部屋には補助講師を 1 名配置し、コミュニケーションツールのトラブル等に対応できるようにした。図 6 にサービス運営組織用、データセンター用の部屋のレイアウトを示す。各テーブルには IP 電話機及び IP Messenger[7] の動作するノートパソコンを配置し IP 電話機はファシリテータからのイベント通知受信用、IP Messenger はサービス運営組織とデータセンターのコミュニケーションチャネルとした。また IP Messenger はサービス運営組織、データセンター、ファシリテータのグループチャットで連絡することでファシリテータがコミュニケーションの状況を確認できるようにした。また今回の実施ではトレンドマイクロ株式会社が公開しているインシデント対応ボードゲームのイベントカード及びアクションカードを使用した。各テーブルにはアクションカードが配置されている。アクションカードは事前にサービス運営組織とデータセンターの持つ役割に応じて振り分けた。サービス運営組織とデータセンターの持つ役割を表 1 及び表 2 に示す。例えば『社員教育を行う』というアクションは人

事で行うアクションと考えられるため当該アクションカードは人事の役割を持つサービス運営組織のイベントカードとする。

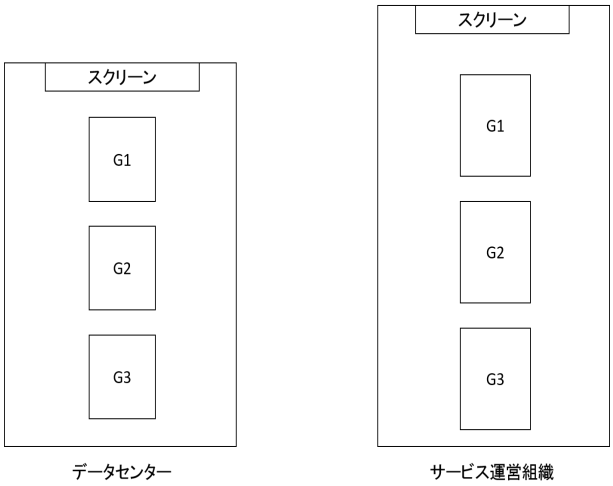


図 6　各部屋のレイアウト

図 7　ファシリテータの様子

表 1　サービス運営組織の役割

役職	行動内容	備考
取締役	経営判断を行う	
コールセンター	社外からの問合わせ窓口を担当	
広報	インシデント対応について顧客やメディアに説明	
情報システム本部	導入機器の選定や運用方針の決定を行う	機器の操作はデータセンター組織に指示を出す
総務	情報システム監査を実施	
人事	社員教育を実施	

表 2　データセンターの役割

役職	行動内容	備考
情報システム部	社内システムや Web 通販サービスの開発、構築、保守	
オペレーション事業部	社内システムや Web 通販サービスのオペレーション	

図 7 にファシリテータ用の部屋の様子を示す。3 名のファシリテータを用意し、それぞれ担当するグループを決定した。各ファシリテータのテーブルには IP 電話機及び IP Messenger の動作するノートパソコンを配置し IP 電話機はサービス運営組織又はデータセンターへのイベント通知用、IP Messenger はサービス運営組織とデータセンターのコミュニケーションチャネル確認用とした。また各ファシリテータのテーブルにイベントカード及び各イベントカードに対する台詞を配置した。イベントカードは事前に表 1 及び表 2 で示したサービス運営組織とデータセンターの持つ役割に応じて振り分けた。例えば『顧客からの電話でコールセンターがパンク』というイベントはコールセンターで発生するイベントと考えられるため当該イベントカードはコールセンターの役割を持つサービス運営組織のイベントカードとする。

各プレイヤーの所属する会社は株式会社 KO とした。株式会社 KO の設定を下記に示す。

- Web 通販の大手グローバル企業
- モバイル端末と連携した革新的な Web 決済システムを開発し自社通販サイトへの導入直前
- 年間売上高 500 億円 ・ 従業員数 300 人
- 業界内では大きな事業規模を誇るがセキュリティは『あと一歩足りない』
- 工業部品などを販売するプロ向けの Web 通販サイトを運営しており、
- ネット決済も行っているが PCI-DSS を取得していない。
- 外部への Web アクセスは「プロキシログ」を 3 か月分程度保管している
- Windows 2012 R2 Server で Active Directory を構成している
- WindowsXP・Windows 2003 Server も一部で残っている
- UTM・ネットワークセンサー・次世代 FW は導入されていない
- 資産管理は番号シールを貼り付け行っているが野良端末も多数あり、詳細不明
- セキュリティ対策は、メールのスパムフィルタ、アプライアンスの IDS のみ。

- 現在いずれも異常検出時の決まった運用は無い
- WSUS で Windows Update のみ配信しているがその他はユーザ任せ
- 導入されているセキュリティ製品は企業向けエンドポイントのウイルス対策ソフトのみ

株式会社 KO のシステム構成を図 8 に示す。

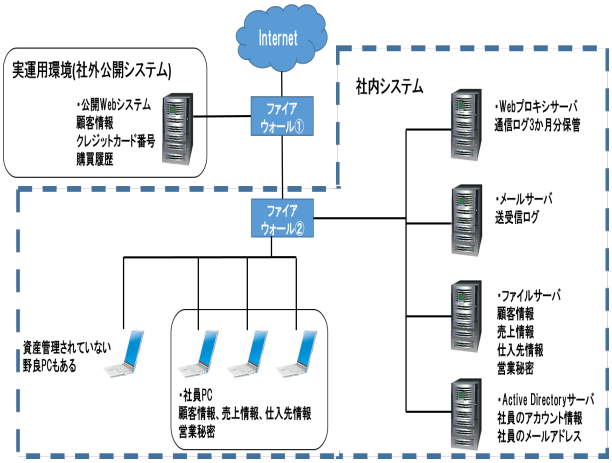


図 8　株式会社 KO のシステム構成

6.2　演習スケジュール

2017 年 12 月 21 日に開催した演習は 3 時間の内容とし、下記スケジュールで実施した。

13:00-13:20
　演習の狙い及び進め方の説明

13:20-13:50
　自己紹介・設定の確認・グループ、担当決め・部屋移動、動作確認

13:50-14:10
　イベント発生・アクション検討フェーズ

14:10-14:20
　アクション決定フェーズ

14:20-14:30
　休憩及び部屋移動

14:30-14:40
　フィードバックフェーズ及び解説

14:40-15:00
　各グループでラウンド 1 振り返り及び部屋移動

15:00-15:15
　イベント発生・アクション検討フェーズ

15:15-15:25
　アクション決定フェーズ

15:25-15:35
　部屋移動

15:35-15:50
　フィードバックフェーズ：気付きの共有

15:50-16:00
　まとめ・アンケートのお願い

サービス運営組織用の部屋をメイン会場とし、参加者全員に対して説明を行う場合はサービス運営組織用の部屋へ参加者全員を収容し説明を行った。演習冒頭は演習の目的や実施内容の流れ等について全員へ説明するためサービス運営組織用の部屋へ全員収容し説明を行った。また各グループ内でサービス運営組織とデータセンターの所属者を決めた。各グループで所属が決まるとデータセンター所属の参加者はデータセンター用の部屋へ移動し、機器の動作確認などを行った。その後 1 回目のゲームが開始し、各参加者はコミュニケーションをとりイベントに対する最適なアクションを決定する。アクション決定フェーズが終了するとデータセンター所属の参加者は再度サービス運営組織用の部屋へ移動し、ファシリテータからのフィードバックや講師からの解説をもとに 2 回目のゲームに向けた振り返りをグループ内で行う。振り返りをもとに 2 回目のゲームを実施し、各グループごとに気付きなどを最後に共有する。なお本実施では 1 回目のイベント発生・アクション検討フェーズの制限時間を 20 分とし、2 回目のイベント発生・アクション検討フェーズの制限時間を 15 分とした。

6.3　実施結果と考察

2 回実施した際の各グループのイベント通知からアクションを決定するまでの時間を表 3 に示す。グループ 1 は組織間の連絡を行うチャットの不具合があり、アクション検討時間を大幅に超過しての決定となっているが、いずれのグループについても 1 回目と 2 回目でアクションを決定するまでの時間が軽減していることがわかる。システムやゲームの流れに対する慣れも大きく影響していると考えられるものの、チャットのログを見ると 2 回目は各グループごとに連絡ルールを決めるなど工夫をしていることも影響したことが伺える。

表 3　アクション決定時間の変化

グループ	1 回目の決定時間	2 回目の決定時間
グループ 1	25 分	16 分
グループ 2	17 分	12 分
グループ 3	21 分	12 分

また参加者には図 10 に示すアンケートを実施した。アンケート結果を図 9 に示す。図 9 の a は negative、b は weak negative、c は weak positive、d は positive を示す。

アンケート結果を見ると演習環境の満足度と演習で学んだ技術の実践力が高くなったと感じますか？について 23%が weak negative を示している。演習環境の満足度についてはグループ 1 でチャットのトラブルがあったことや、既存のソフトを利用したことによってインタフェース

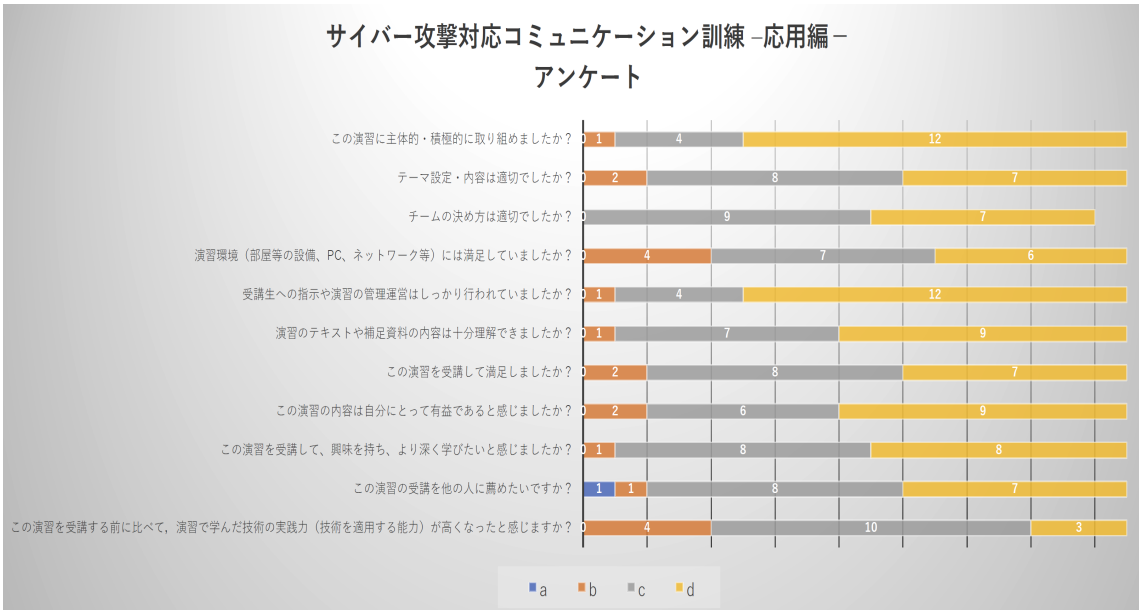
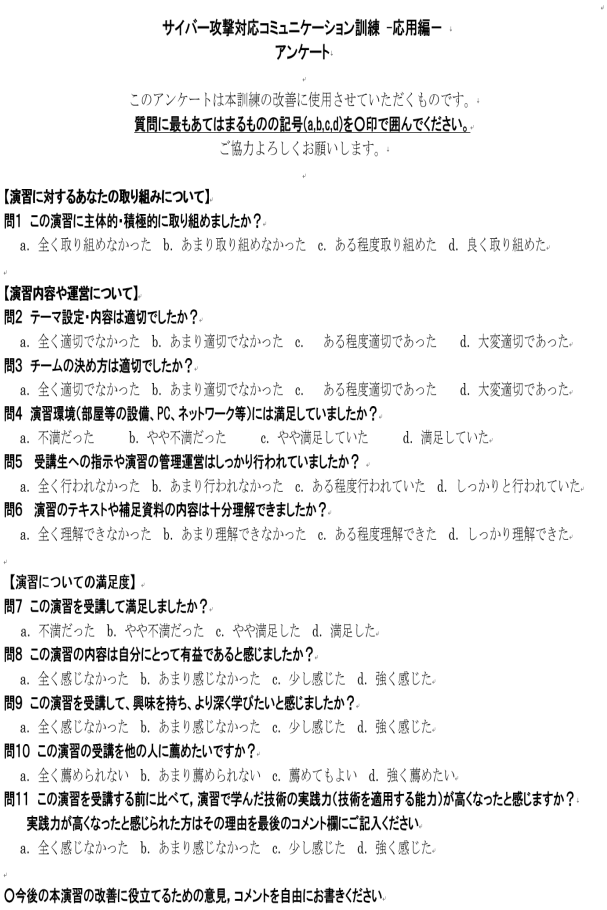


図 9　アンケート結果



サイバー攻撃対応コミュニケーション訓練 –応用編–
アンケート

このアンケートは本訓練の改善に使用させていただくものです。
質問に最もあてはまるものの記号(a,b,c,d)を○印で囲んでください。
ご協力よろしくお願いします。

【演習に対するあなたの取り組みについて】
問1 この演習に主体的・積極的に取り組めましたか？
a. 全く取り組めなかった b. あまり取り組めなかった c. ある程度取り組めた d. 良く取り組めた

【演習内容や運営について】
問2 テーマ設定・内容は適切でしたか？
a. 全く適切でなかった b. あまり適切でなかった c. ある程度適切であった d. 大変適切であった
問3 チームの決め方は適切でしたか？
a. 全く適切でなかった b. あまり適切でなかった c. ある程度適切であった d. 大変適切であった
問4 演習環境(部屋等の設備、PC、ネットワーク等)には満足していましたか？
a. 不満だった b. やや不満だった c. やや満足していた d. 満足していた
問5 受講生への指示や演習の管理運営はしっかり行われていましたか？
a. 全く行われなかった b. あまり行われなかった c. ある程度行われていた d. しっかりと行われていた
問6 演習のテキストや補足資料の内容は十分理解できましたか？
a. 全く理解できなかった b. あまり理解できなかった c. ある程度理解できた d. しっかり理解できた

【演習についての満足度】
問7 この演習を受講して満足しましたか？
a. 不満だった b. やや不満だった c. やや満足した d. 満足した
問8 この演習の内容は自分にとって有益であると感じましたか？
a. 全く感じなかった b. あまり感じなかった c. 少し感じた d. 強く感じた
問9 この演習を受講して、興味を持ち、より深く学びたいと感じましたか？
a. 全く感じなかった b. あまり感じなかった c. 少し感じた d. 強く感じた
問10 この演習の受講を他の人に薦めたいですか？
a. 全く薦められない b. あまり薦められない c. 薦めてもよい d. 強く薦めたい
問11 この演習を受講する前に比べて，演習で学んだ技術の実践力(技術を適用する能力)が高くなったと感じますか？
実践力が高くなったと感じられた方はその理由を最後のコメント欄にご記入ください
a. 全く感じなかった b. あまり感じなかった c. 少し感じた d. 強く感じた

○今後の本演習の改善に役立てるための意見，コメントを自由にお書きください

図 10　アンケート

として使用し難い部分があったことが影響したと考えられる。今後は制限時間表示、チャットなど本演習で必要となる機能を統合したシステムを構築することなどでトラブルの軽減やユーザビリティ向上が望める。実践力については一部の人に演習の目的が明確に伝わっていなかった部分が影響したと考えられる。そのため目的の明確化とともに目的を明確に伝えるため何度も明示するなどの工夫を行う必要がある。

今回の実施では要求スキルを低くするため電話対応のみを導入したが、例えばWebサーバやサーバログを演習環境に用意することでWebの改ざんが発生した際に事実確認が出来るようにしたり、対象者に合わせてより現実に近い環境でのコミュニケーション訓練への応用も考えられる。

7. 結論

本稿ではサイバーセキュリティインシデント発生時における組織間コミュニケーション訓練のための演習設計とその評価について述べた。サイバーセキュリティインシデントの増加に伴い組織においてサイバーセキュリティインシデントが発生した場合に備えた対応手順などの策定が進んでいる。また、実際に発生した場合に備えて研修や対応訓練などが行われている。特にサイバーセキュリティインシデントは組織内における特定の専門家のみが対応出来れば良いものではなく、物理的に離れた場所に居る人も含め様々なロールの人が連携して迅速に対応する必要がある。そのためには各組織に合致した状況で繰り返し組織間を跨ぐコミュニケーションの訓練が重要となる。これまでも多くのサイバーセキュリティインシデント対応訓練が開発されているが、その多くは専用の設備を必要としたり、準備コストが高く、容易に実施することが困難である。近年容易に繰り返し実施可能なゲーム形式の訓練も登場してきているがその多くは一同に会して実施するものが多く、組織間コミュニケーションの訓練となるものは少ない。そこで本研究では物理的に離れた場所にある組織間のコミュニケーションも考慮したサイバーセキュリティインシデント

対応演習を設計し、実際にその様な状況での対応も想定される企業で実施した。実施した結果、繰り返し訓練することで対応にかかる時間短縮や対応手順の洗練などを確認出来たほか、参加者から演習が実践的な演習となっていたこともアンケート結果からわかった。

参考文献

[1] SecCap. https://www.seccap.jp/.

[2] SecCap コースの演習科目群. https://www.seccap.jp/gs/course/practice.

[3] 第12回情報危機管理コンテスト. http://www.riis.or.jp/symposium21/crisismanagement/purpose/.

[4] Kaspersky. http://www.kaspersky.co.jp/enterprise-security/cybersecurity-awareness.

[5] Trendmicro. https://www.trendmicro.com/ja$_j p/security-intelligence/research-reports/learning.html$.

[6] JNSA. http://www.jnsa.org/edu/secgame/secwerewolf/secwerewolf.html.

[7] IP Messenger. https://ipmsg.org/.

[8] Masato Yamanouchi, Kozue Nojiri, and Hideki Sunahara. A remote security exercise system for beginners considering scalability and simplicity. In *The Second Asian Conference on Defence Technology The First Pacific Rim International Workshop on Defence, Safety, and Security Technology(ACDT2016)*, Jan 2016.

[9] Tomomi Aoyama, Toshihiko Nakano, Ichiro Koshijima, Yoshihiro Hashimoto, and Kenji Watanabe. On the complexity of cybersecurity exercises proportional to preparedness. *Journal of Disaster Research Vol*, Vol. 12, No. 5, p. 1081, 2017.

[10] Tomomi Aoyama, Kenji Watanabe, Ichiro Koshijima, and Yoshihiro Hashimoto. Developing a cyber incident communication management exercise for ci stakeholders. In *International Conference on Critical Information Infrastructures Security*, pp. 13–24. Springer, 2016.