LAC

情報セキュリティ事故対応 1日コース 机上演習編

実践的な演習を通して事故対応の
本質に迫る「気づき」が得られます

疑似的に事故対応を体験しておくことで実際の事故の際、臨機応変に対応できます

セキュリティアカデミー
講師 **大塚英恵**

情報セキュリティ事故のための対応手順や対応チーム（CSIRT※）の整備において、重要なのは「臨機応変に対応できるか」の確認です。立派なマニュアルを策定していても、それが有効に活用されなければ意味がありません。

そこで必要とされるのが体験による「気づき」です。本コースは、予告なしにインシデント情報を伝え、それに対するアクションによって状況がめまぐるしく変わるという、練りに練ったシナリオで進む机上演習です。実際に起きた重大なインシデントを基に構成したシナリオで事故対応を体験することで、自分で考え判断し、行動する力の必要性、加えてチームや社内外との連携の大切さ、難しさを体感していただけます。この体験を通した「気づき」が、組織の情報セキュリティ事故対策に必ず役立つと自信を持っています。

情報セキュリティ事故対応に携わる担当者、CSIRT、情報システム部門の方々、危機管理委員会や組織マネジメント層、広報、法務部などの方々にもお勧めいたします。

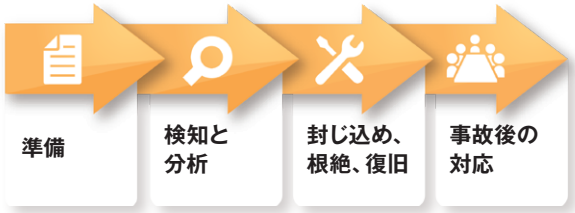
※CSIRT（Computer Security Incident Response Team）＝コンピューターセキュリティに関する事故対応チーム

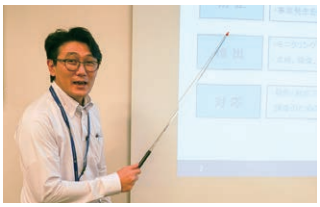
研修当日スケジュール

時間		内容	
10:00～	60分	1 座学	インシデントレスポンス概論
11:00～	60分	2 ルール説明	訓練の進め方と前提条件の説明
12:00～	60分	休憩	
13:00～	150分	3 訓練	インシデントレスポンス訓練
		途中休憩あり	
15:45～	45分	4 振り返り	グループ別ディスカッション
16:30～	60分	5 発表	全体発表・まとめ

1 座学
「インシデントレスポンス概論」

そもそもインシデントレスポンスとは何か、インシデントにどう対応するべきかを座学で学習します。インシデントレスポンスを４つのフェーズに分けて、それぞれの目的を明確にするとともに、原因の調査や組織内外へのアプローチにおいてどのように行動すべきかを体系的に学ぶことで、対応ポイントの知識を得ることができます。





2 ルール説明
「訓練の進め方と前提条件の説明」

訓練は、発生した事象と仮想組織の資料を利用して、事故の収束と復旧、また再発防止策の検討をシミュレーションスタイルで行います。受講者はCSIRTとして、４～７人でチームとなって対応。訓練を開始する前に、仮想組織の概要やシステムおよびネットワークの構成といった前提条件を確認して訓練に参加します。

受講者（CSIRT）
仮想組織のCSIRTメンバーとしてインシデントを対処します

第一報　事故の発生を予感させる情報

アクション　与えられた情報が本当に事故かどうかの分析を行い、情報収集や対策といったアクションを講師に対して行う

回答　アクションに基づき各種の情報を返答

以降、回答を基にフェーズに沿ってインシデントレスポンスを進め、復旧を目標に対応します

講師
CSIRT以外のすべての役を演じます
取引先、顧客、経営者、社員、ベンダー、警察、マスコミ etc.

さあ、訓練を始めましょう！
あれ、不審なメールが届いたみたいですよ…

次ページへ

3 訓練「インシデントレスポンス訓練」

訓練シナリオは、スタートするまで開示されません。受講者はCSIRTの一員として情報を受け、メンバーと対応方針を決定し、関係者（講師が複数兼任）と連絡を取り合いながら、インシデントの原因、被害状況を特定、事業の復旧を目指します。よって、展開や結果がチームのアクションによって異なるのがこの訓練の醍醐味。ここでご紹介するのはその一例です。

story CSIRTの定例会議中、「社内で違和感のあるメールを受信した人がいるようだ」という、もやっとした情報が寄せられます

mission 1 インシデントの検知と分析

舞い込んだ情報は事実か？　すでに問題が発生しているのか？　現状把握のため「依頼票」を使って調査を開始。複数の人が同様のメールを受け取っていることが判明したので、メールの正体の追究に着手しました。

POINT
対応時間の短縮が被害の最小化につながります。チームでコミュニケーションを取って積極的にアクションし、効率的に情報を収集できるかがポイントです。

mission 2 封じ込め・根絶

メールの正体の追究と同時に、被害をこれ以上広げない対策にも着手しました。

POINT
原因調査をする前に、まずは被害を拡大させないための封じ込めを優先することが大事です。

story　ここで新たな問題発生！　情報漏洩が疑われる報告が上がりました

mission 3 インシデントの検知と分析

最初と同様に真偽や現在の被害状況を把握するとともに、2つの問題は無関係なのか、関連しているならどの部分か、さらに被害を最小限に抑えるにはどうすればよいか、チーム内でさまざまな意見を出し合い、その都度、アクションを起こしました。

POINT
あらゆる状況や原因を想定しましょう。経営者や外部にいつ伝えるかも大きなポイント。アクションの有無が流れを変えます。

mission 4 封じ込め・根絶

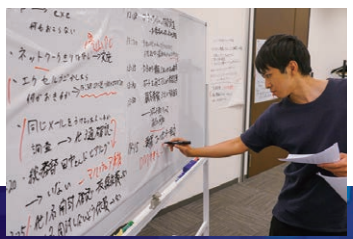
次々にやるべきことが増えて、ややパニック。事業を継続するか、一旦ストップするかでメンバーの意見が割れ、行き詰まる場面も。

POINT
作業分担などチームワークが必須。情報や状況をホワイトボードなどで整理し、共有することが大事です。

mission 5 復旧

インシデントで迷惑をおかけした取引先や顧客に対するお詫びの仕方と、早急な事業再開の手段を考えました。

POINT
これまでの対応によってクレームが殺到することも。常にビジネスに対する損失を考慮して対応しましょう。



4 振り返り

訓練終了後、対応の方法や内容が適切だったかを振り返り、得られた気づきを発表できるように議論してまとめます。

5 発表

振り返りのまとめを各チームの代表が発表します。さまざまな方法や考え方があることが理解でき、気づきが広がります。

A チーム

想定外の事象のなかには不確かな情報も紛れていて、先入観だけでは本当に危ないことを実感できました。
もし自社で起きたらと思うとゾッとしました。

B チーム

演習が進むにつれ、社内・社外対応が重要なことを感じました。
特に、社外対応がうまくできませんでしたが、逆に失敗した際のクレーム対応などが経験できてよかったです。

C チーム

焦る状態での判断ミスや難しさをよく認識できました。
当たり前だろうという対処も、実行するとなると考えるべきことがたくさんあり、できないことが多かったです。

Message

セキュリティアカデミー
講師
白井雄一郎

各チームに１人ずつ講師が付き、アクションや状況によっても対応がさまざまですから、同じ１本のメールから始まったインシデントでも、収束への道筋、着地点が異なります。それには正解も間違いもありません。大事なのはこの演習を通じて、どれだけの気づきが得られたかです。

Voice

教育ご担当者様の声

新任のCSIRT要員はもちろん一般社員にも、いざセキュリティインシデントが発生したときにどのような対応が必要かを実践的に学ぶ機会が必要と考え、受講を勧めました。セキュリティ関連はとっつきにくいイメージがありましたが、「楽しい演習だった」と、良い反応が返ってきており、実際、日々の業務においてもセキュリティへの関心が高まったと感じています。また、演習で扱ったセキュリティ事故が実際に発生した場合に備え、受講で得た学びを活かして、インシデント対応マニュアル、チェックリストなどの見直しを実施することもできました。今後も、参加者を変更しながら、継続して受講させたいと考えています。

受講者様の声

- 座学でインシデント対応の基礎から一連の動きをわかりやすく学んで演習に入ったので、理解しやすかったです。
- 脱出ゲームのような訓練でとても楽しく勉強することができました。
- その場で、自分たちで考えアプローチをすることによって理解が深まりました。
- 講師の「こういう場合はどう対応する？」という視点+アドバイスが明確。答えを教えるのではなく、答えが出るように導いていただけ、とてもよい勉強になりました。
- 実際にインシデントが起きたときは、CSIRTメンバーだけではなく、いろいろな部署との連携が大切だと気づきました。
- 実践を意識できる緊張感がある演習でした。
- インシデントハンドリングでは、技術面の追求だけではなく事業継続や対外対応といった観点も重要だということに気づけました。
- インシデントの内容によっては、影響範囲が広くまた相当な期間にわたり影響が続く可能性が高いことに気づかされました。
- 事故が起こった時、多くの人が関わること、決断を下す責任の大きさが分かり、2手3手先を見据えた行動が必要だなと感じました。
- 職場の方や業務をされている方の意見を聞くことで、多種多様なアプローチを見ることができました。選択が「間違い」と一概に判断するのではなく、視野を広げる良い機会でした。

選べる

情報セキュリティ事故対応１日コース 机上演習編

研修&受講スタイル

それぞれ２つの研修形態と受講形態を組み合わせ、
受講者様のニーズによりマッチしたスタイルで受講することができます。

研修形態

■オープン開催

開催日程を設定し、参加募集をして実施する形態です。複数の企業・団体からの受講者が参加されます。

費用：132,000円（税込）／１名

■個別開催

単一企業向けの研修。希望の日程、受講形態をご指定いただく形になります。

※座学パートを事前にオンライン受講（動画）していただくことで、開催時間を短縮することも可能です。

費用：1,320,000円（税込）／１開催（21名まで）

受講形態

■集合研修

弊社会場（永田町）にお越しのうえ、受講していただきます。

■リモート研修

インターネットを利用して、Live配信で受講していただきます。

ラック　事故対応演習　検索

こちらもおすすめ！

情報セキュリティ事故対応２日コース 実機演習編

ファイアウォールやサーバで構成された実機環境を使用し、実際に事故が起きた想定で2日間にわたって演習を行います。

実施内容

１日目……**1. インシデントレスポンス**（座学）
2. ルール説明（訓練説明）
3. インシデントレスポンス実機訓練（1回目）

２日目……**4. 情報セキュリティ最新動向**（座学）
5. インシデントレスポンス実機訓練（1回目）

受講者様の声

- 実機を使用することで、リアルな現場感が高まりました。
- セキュリティの技術だけでなく、心得も学べたので参考になりました。

LAC Security Academy

株式会社ラック　セキュリティアカデミー
〒102-0093 東京都千代田区平河町２丁目16番１号 平河町森タワー
TEL：03-6757-0125　FAX：03-6757-0112
Email：info-academy@lac.co.jp　https://www.lac.co.jp/service/education/