別紙2

サイバー防御演習 説明資料

平成30年9月8日

仙台CTF推進プロジェクト

サイバー防御演習の概要

- 参加者は、架空の企業「株式会社仙台シーテーエフ」の情報セキュリティ対応チームとして、社内で発生するインシデントに対処します。

◆演習のイメージ

事務局が「イベント」を提示

イベント

チームで対応を検討

＋

必要に応じて、配布されたログデータ等を実機で解析

事務局

参加者チーム

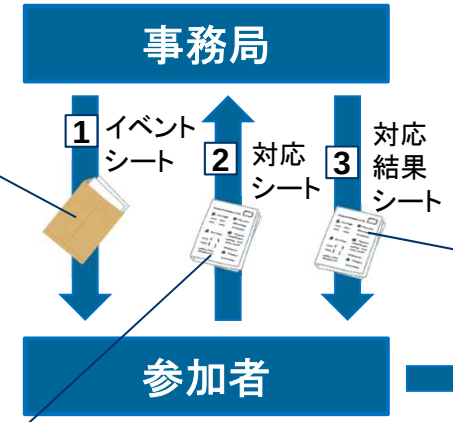
演習の進行方法

- 参加者は、事務局から提示される「イベント」に対して、状況終了と判断するまで「検討」と「対応」を繰り返してください。
- 対応中に新たなイベントが発生した場合は、優先度が高いと判断したイベントの対応に切り替えて構いません。

1 イベントフェーズ

・事務局は、時間経過に応じて、参加者に「イベント」シートを配布

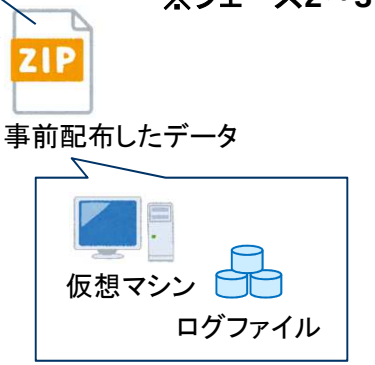
［イベントの例］
営業所の社員用PCでウイルス検知アラートが発生



3 対応フェーズ

・事務局は、アクション応じた「対応結果」シートを参加者に開示（対応シートも返却）
・参加者は、「調査」を選択した場合、必要に応じて事前配布した仮想マシン等の解析を実施
・参加者は、発生した事象、対応結果などを「記録様式」に記録

※フェーズ2～3を繰り返し実施



2 検討フェーズ

・参加者は、事象の推測、対応方針などをチームで相談
・実施すべきアクションを「対応」シートに記載のうえ、事務局に提示

［アクションの例］
①利用者に電話で状況確認
②ログ等の調査
③機器の設定変更
④対応不要・状況収束と判断

様式「イベント」シートのイメージ

イベント

管理番号	E01
発生日時	2018年9月8日（土）13:30
イベントの内容	ウイルス対策ソフトの管理サーバから、検知アラートが通知されました。

検知日時	2018年9月8日 13:30
脅威名	JS_POWLOAD.ELDSAUJQ
検出ファイル名	C:¥Users¥suzuki¥AppData¥Local¥Microsoft¥Windows¥Temporary Internet Files¥Content.Outlook¥BNTENH3O¥請求書.zip
検査の種類	リアルタイムスキャン
処理結果	隔離
検出コンピュータ名	PC0010　IPアドレス：172.16.0.130 ［営業所の社員Aさんが利用しているパソコン］

検知した脅威名など、必要に応じてインターネットで情報検索して判断の参考材料としてください。

様式「対応」シートのイメージ

対応

管理番号	E01-A
状況推測	（メモ欄：発生した事象や想定されるリスクなどについて推測した結果などを記載）
対応方針	（メモ欄：対応すべき事項と優先順位などを記載）
アクション	（以下の選択肢から一つだけ選択し、選択した順番を記載。実技以外は、同じアクションを2回選択することはできない） 1 （1）利用者（スズキさん）に電話連絡し状況を確認 □ （2）隔離された検体の調査［実技］ □ （3）対応不要・状況終了

参加者チームで相談した内容を記載するメモ欄

1番最初に実施すべきアクションに「1」を記載し事務局に提示
※対応結果シートを受け取った後、別のアクションを選択する場合は、「2」を記載。以降、選択した順番の数字を記載

「対応結果シート」に、演習データのファイル名が記載してあります。
※実技調査は、何回でも実施可

様式「対応結果」シートのイメージ

対応結果

管理番号	E01-A-R01　[選択したアクション：(1) 利用者（スズキさん）に電話連絡し状況を確認]
対応結果	Aさんに電話連絡したところ、社外の取引先と思われるアドレスから届いたメールの添付ファイルを開封しようとしたところ、セキュリティの警告が出たので操作を中断したとのこと。 [メールの概要] 件名：請求書を送ります 本文：いつもお世話になっております。6月分請求書リストが出来ましたので、添付いたします。 オリジナルは、明日の朝一必着で郵送手配いたします。 添付：請求書.zip
状況推測	（メモ欄：対応結果を踏まえ、発生した事象や想定されるリスクなどを記載） 参加者チームで相談した内容を記載するメモ欄
次のアクション	（メモ欄：対応結果を踏まえ、追加で対応すべき事項などを記載）

様式「記録様式」のイメージ

時刻	発生した事象、対応などの記録
:	
:	
:	
:	
:	
:	
:	
:	
:	
:	
:	
:	

参加者チームで相談、判断した
日時と内容を記録してください。

演習のルール

1. **原則として、チーム全員で相談・確認しながら一つずつ対応を進めてください。**
   - 本番のインシデントでは、手分けをして同時並行で作業を進めますが、本演習は学習を目的としているため、全員で相談しながら進めてください。
   - ログ調査などの実技は、作業を手分けしても構いませんが、調査結果は全員で共有してください。

2. **「対応」シートの「アクション」として、ログ調査など実技を行うものは、「対応結果」シートで指定された演習データ（ファイル名）に対して、実機で調査を実施してください。**
   - 「対応結果」シートで指定されていない演習データの調査はしないでください。