仙台CTF2018 Day-1 セキュリティ技術勉強会
サイバー防御演習のシナリオ

経過時間（分）	管理番号	分類	内容
5:00	E01	イベント	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。 検出日時: 2018年9月8日 16:05 脅威名: MAL_OTORUN2 検出ファイル名: E:¥autorun.inf （補足:外部記憶媒体のドライブ名） 検査の種類: リアルタイムスキャン 処理結果: 削除 検出コンピューター名 PC0012、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］
	E01-A	対応	□ (1) 社員Aさんに電話連絡し状況を確認（USBメモリの所有者、他のパソコンへの接続有無など、取り扱いの状況） □ (2) 社員Aさんに電話連絡し、パソコンをネットワークから切り離すよう指示 □ (3) 対応不要・状況終了
	E01-A-R01	結果	選択したアクション:(1)利用者に電話連絡し状況を確認（USBメモリの所有者、他のパソコンへの接続有無など、取り扱いの状況） 社員Aさんから以下の回答がありました。 ・健康セミナー講演のために招聘した外部講師の先生が、当社が準備した発表用パソコン（社員用パソコン）にプレゼン資料をコピーするため、持参したUSBメモリを接続した際に、ウイルス検知アラートが発生した。 ・当該USBメモリは、他のパソコンなどには接続していない。 ・USBメモリは先生の私物であり、当社で調査することはできない。 ・先生とは委託関係はなく、当社の業務データはお渡ししていない。今回の講演料は、謝礼金という形でお渡しする。
	E01-A-R02	結果	選択したアクション:(2) 社員Aさんに電話連絡し、パソコンをネットワークから切り離すよう指示 社員Aさんに連絡し、検知アラートが通知されたパソコンをネットワークから切り離してもらいました。
	E01-A-R03	結果	選択したアクション:(3) 対応不要・状況終了 特に何も起こりませんでした。

経過時間（分）	管理番号	分類	内容
10:00	E02	イベント	営業所の社員Bさんからユーザーサポート部門に電話連絡がありました。 ・パソコンが突然、真っ黒な画面になり、英語のメッセージが表示された。 ・パソコンに格納しているファイルが全て壊れてしまい、困っている。
	E02-A	対応	□ (1) 社員Bさんに電話連絡し状況を確認（事象が発生した前後の状況、英語のメッセージの内容） □ (2) 営業所のシステム担当者に電話連絡し、WANネットワークを切り離すよう指示（営業所外部との通信を全て遮断） □ (3) 社員Bさんに電話連絡し、パソコンをネットワークから切り離すよう指示 □ (4) 不審メールを受信した社員に電話連絡し、不審メールを開封しないよう指示 ［選択の前提条件］不審メールを受信した社員を特定できていること □ (5) システム運用会社に連絡し、メールサーバログを調査し、不審な添付ファイルが付いたメールを受信した社員を特定するよう指示 ［選択の前提条件］不審な添付ファイルの名前を特定できていること □ (6) 営業所のシステム担当者に連絡し、事象発生パソコンの簡易証拠保全を実施し、エビデンスを本社の調査用共有フォルダに格納するよう指示 □ (7) 対応不要・状況終了
	E02-A-R01	結果	選択したアクション：(1) 利用者に電話連絡し状況を確認（事象が発生した前後の状況、英語のメッセージの内容） 社員Bさんから以下の回答がありました。 ・突然、パソコンの画面に英語のメッセージが表示された。何をしてそうなったのか分からない。 ・デスクトップに保管していた「業務情報.txt」が壊れてしまい、ランダムなファイル名となってしまった。内容を確認したが文字化けしている。
	E02-A-R02	結果	選択したアクション：(2) 営業所のシステム担当者に電話連絡し、WANネットワークを切り離すよう指示（営業所と外部との通信を全て遮断） 営業所のシステム担当者に作業を指示しました。作業完了まで20分程度かかるとのことです。
	E02-A-R03	結果	選択したアクション：(3) 社員Bさんに電話連絡し、パソコンをネットワークから切り離すよう指示 社員Bさんに連絡し、事象が発生したパソコンをネットワークから切り離ししました。
	E02-A-R04	結果	選択したアクション：(4) 不審メールを受信した社員に電話連絡し、不審メールを開封しないよう指示 ［選択の前提条件］不審メールを受信した社員【Cさん、Dさん】を特定できていること 社員Cさん、Dさんに連絡し、不審メールを開封する前に削除してもらいました。
	E02-A-R05	結果	選択したアクション：(5) システム運用会社に連絡し、メールサーバログを調査し、不審な添付ファイルが付いたメールを受信した社員を特定するよう指示 ［選択の前提条件］不審な添付ファイルの名前【請求書.zip】を特定できていること システム運用会社に連絡し、調査を指示しました。 調査の結果、社員Cさん、Dさんも不審メールを受信していることが判明しました。 ⇒ アクション(4)を選択できるようになりました。
	E02-A-R06	結果	選択したアクション：(6) 営業所のシステム担当者に連絡し、事象発生パソコンの簡易証拠保全を実施し、エビデンスを本社の調査用共有フォルダに格納するよう指示 営業所のシステム担当者から、今ほどエビデンスを共有フォルダに登録したとの報告がありました。 ［実技］エビデンス（/var/samba/public/exercise）を解析し、感染原因を推測してください。 ヒント：感染原因となった可能性がある「不審なメール添付ファイル」の名前を特定してください。 （注記）実習データ準備の都合上、2018年8月25日（土）11:00頃に利用者から通報を受けたという前提で調査してください。 ⇒感染原因となった可能性がある「不審なメール添付ファイル」の名前を特定すると、アクション(5)を選択できるようになります。
	E02-A-R07	結果	選択したアクション：(7) 対応不要・状況終了 アクション(4)を実行済みの場合 皆さんの対応により、ランサムウェアの感染被害を最小限に抑えることができました。 社員Bさんのパソコンに格納されていたデータはランサムウェアにより破壊されたものの、バックアップから復旧することができました。 アクション(4)を未実行の場合 社員Cさん、社員Dさんからも、画面に不審なメッセージが表示され、ファイルを開けなくなったとの通報がありました。