2017年11月12日（日）開催予定 仙台CTF
参加予定者向け事前案内資料

仙台CTFの概要と
参加者の事前準備について

2017年9月18日

（2017年11月3日修正）

仙台CTF実行委員会

本書について

- 本書は、仙台CTF参加予定者向けの事前案内資料です。

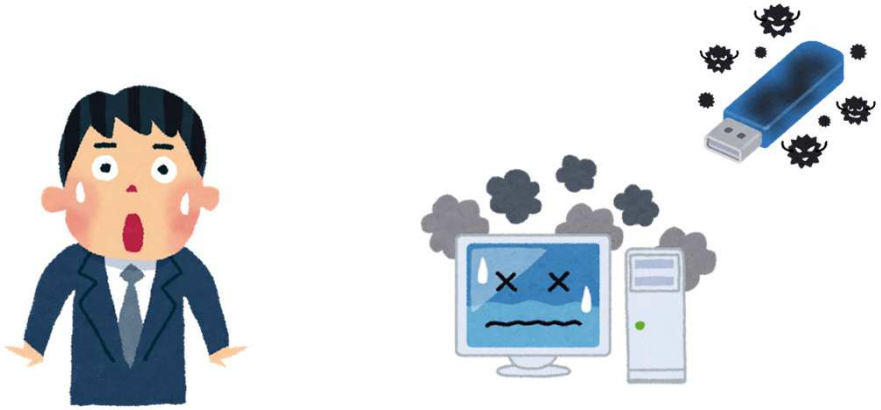
- 「セキュリティ技術勉強会」、および「セキュリティ技術競技会（CTF）」をスムーズに進めるための参考情報が記載されていますので、ぜひご一読ください。

目次

1.仙台CTFの舞台設定

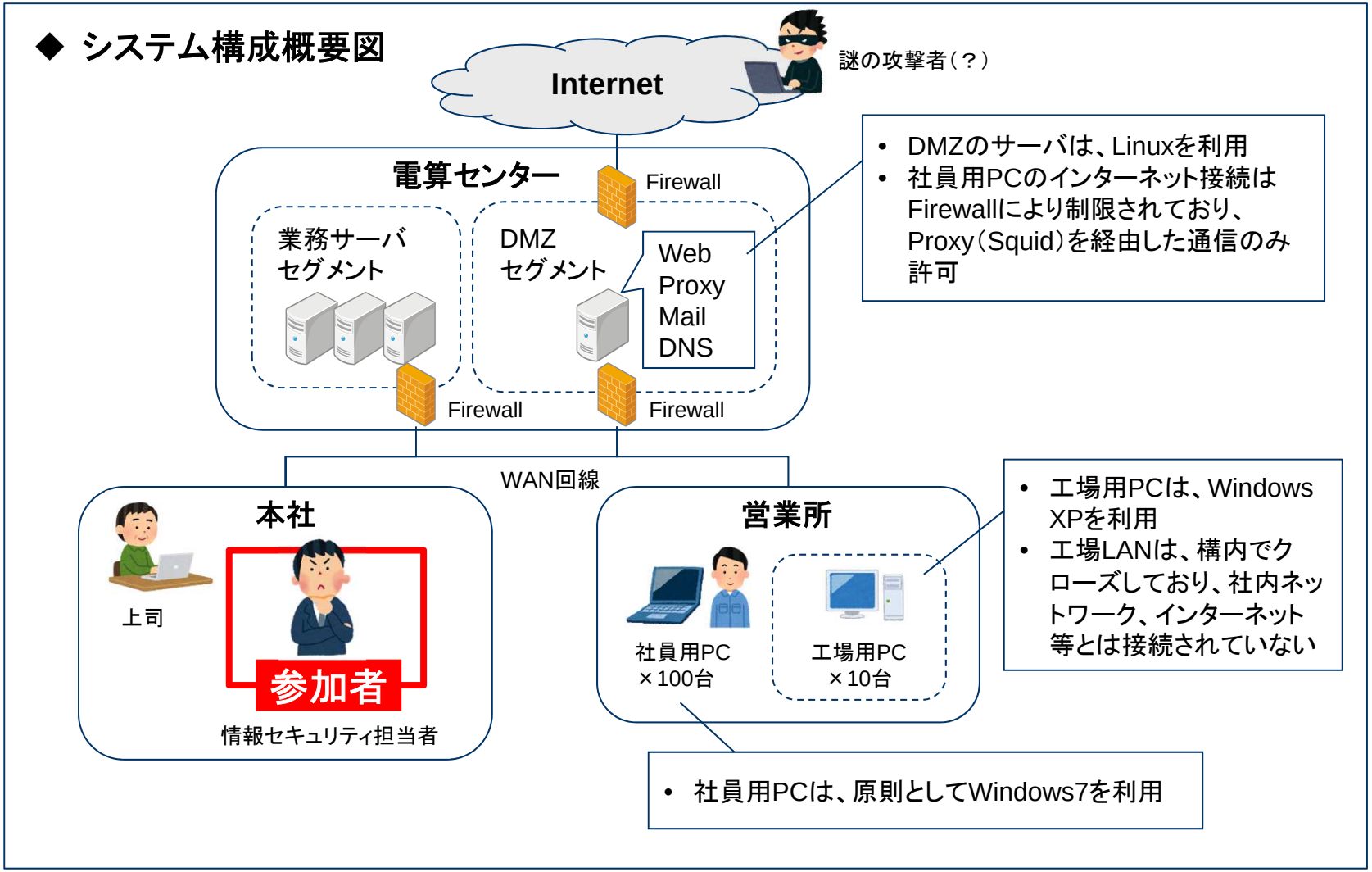
仙台CTFの舞台設定

- 技術勉強会、技術競技会のいずれも、架空の企業「株式会社仙台シーテーエフ」を舞台としています。
- あなたは、「株式会社仙台シーテーエフ」に入社したばかりの新米情報セキュリティ担当者です。先輩と2人で業務を進めていましたが、先輩が怪我で入院してしまったため、社内の情報セキュリティに関するさまざまな問題に一人で対処することになりました。



「株式会社仙台シーテーエフ」のシステム構成

◆ システム構成概要図



2.セキュリティ技術勉強会の概要と事前準備

セキュリティ技術勉強会の概要

- **「株式会社仙台シーテーエフ」で発生したインシデントを題材としたシナリオに沿って、調査・対応の基本手順について、実習を交えて学習します。**

シナリオ

- IDS（不正侵入検知装置）のアラートにより、営業所の社員用PCがインターネットに不審な通信を発信していることが判明しました。
- あなたは、社員用PCがマルウェアに感染している可能性が高いと考え、調査・対応を実施することとしました。

学習内容

- インシデント対応の基本手順
- プロキシサーバのログ調査
- パソコンのメモリ保全
- メモリフォレンジック
- タイムライン解析
- 感染の影響調査

学習目標

- パソコンのメモリイメージを解析し、不審通信を発生させているプロセスを特定できる。
- パソコンのディスクイメージをタイムライン解析し、感染原因となった挙動を特定できる。

セキュリティ技術勉強会の事前準備(1)

- **勉強会で利用する次のソフトウェアを事前にインストールしておいてください。**

(1)テキストエディタ

- サクラエディタ、vimなど、お好みのテキストエディタをご準備ください。

(2)Volatility Framework

① 公式サイト※1から、ご利用しているOS版の「Standalone Executable」のZIPファイルをダウンロードし、任意のフォルダに展開してください。(下図の実行例では、c:¥workに展開しています。)

(※1) http://www.volatilityfoundation.org/releases

② コマンドプロンプトでカレントディレクトリを上記のフォルダに移動し、下図のように「--help」オプションを付けて実行し、「ERROR」などのメッセージが表示されないことを確認してください。

◆「Volatility 2.6 Windows Standalone Executable (x64)」による実行例

```
C:¥>cd c:¥work       (補足) 展開したフォルダ (ここではc:¥work) に移動します。
C:¥work>volatiliey_2.6_win64_standalone.exe --help
Volatility Foundation Volatility Framework 2.6
Usage: Volatility - A memory forensics analysis platform.

Options:
 -h, --help            list all available options and their default values.
                        Default values may be set in the configuration file
 (中略)
                wndscan         Pool scanner for window stations
                yarascan        Scan process or kernel memory with Yara signatures

C:¥work>
```

セキュリティ技術勉強会の事前準備(2)

(3-1)Plaso(log2timeline) [Windows版]

① 公式サイト※2から、32bit版または64bit版の「Plaso 1.5.1」をダウンロードします。
(下図の実行例では、64bit版である「plaso-1.5.1-win-amd64-vs2010.zip」を利用しています。)
(※2) https://github.com/log2timeline/plaso/releases/tag/1.5.1

② ダウンロードしたZIPファイルを任意のフォルダに展開してください。
(下図の実行例では、c:¥workに展開しています。)

③ コマンドプロンプトを起動し、下図のように、インストールしたフォルダに移動したうえで、log2timelineを「-V」オプションを付けて実行し、「ERROR」などのメッセージが表示されないことを確認してください。

◆「plaso-1.5.1-win-amd64-vs2010」による実行例

```
C:¥>cd c:¥work       (補足) 展開したフォルダ (ここではc:¥work) に移動します。
C:¥work>log2timeline -V
plaso - log2timeline version 1.5.1

C:¥work>
```

動作確認済環境:Windows10 Pro 64bit版(Creators Update)

セキュリティ技術勉強会の事前準備(2)

(3-2)Plaso(log2timeline) ［Max OS X版］

① 公式サイト※2から、「plaso-1.5.1-macosx-10.12.dmg」をダウンロードします。
（※2）https://github.com/log2timeline/plaso/releases/tag/1.5.1

② 次の手順でインストールします。

① ダウンロードしたdmgファイルをダブルクリックし、マウントしてください。

② ターミナルから次のコマンドを実行し、インストールします。

```
$ cd /Volumes/plaso-1.5.1
$ sudo ./install.sh
$ sudo easy_install pefile sudo easy_install traitlets pygments pexpect
  backports.shutil_get_terminal_size pathlib2 pickleshare prompt_toolkit simplegeneric
```

③ dmgファイルをアンマウントしてください。

③ ターミナルから、下図のように、log2timelineを「-V」オプションを付けて実行し、「ERROR」などのメッセージが表示されないことを確認してください。

◆「plaso-1.5.1-macosx-10.12.dmg」による実行例

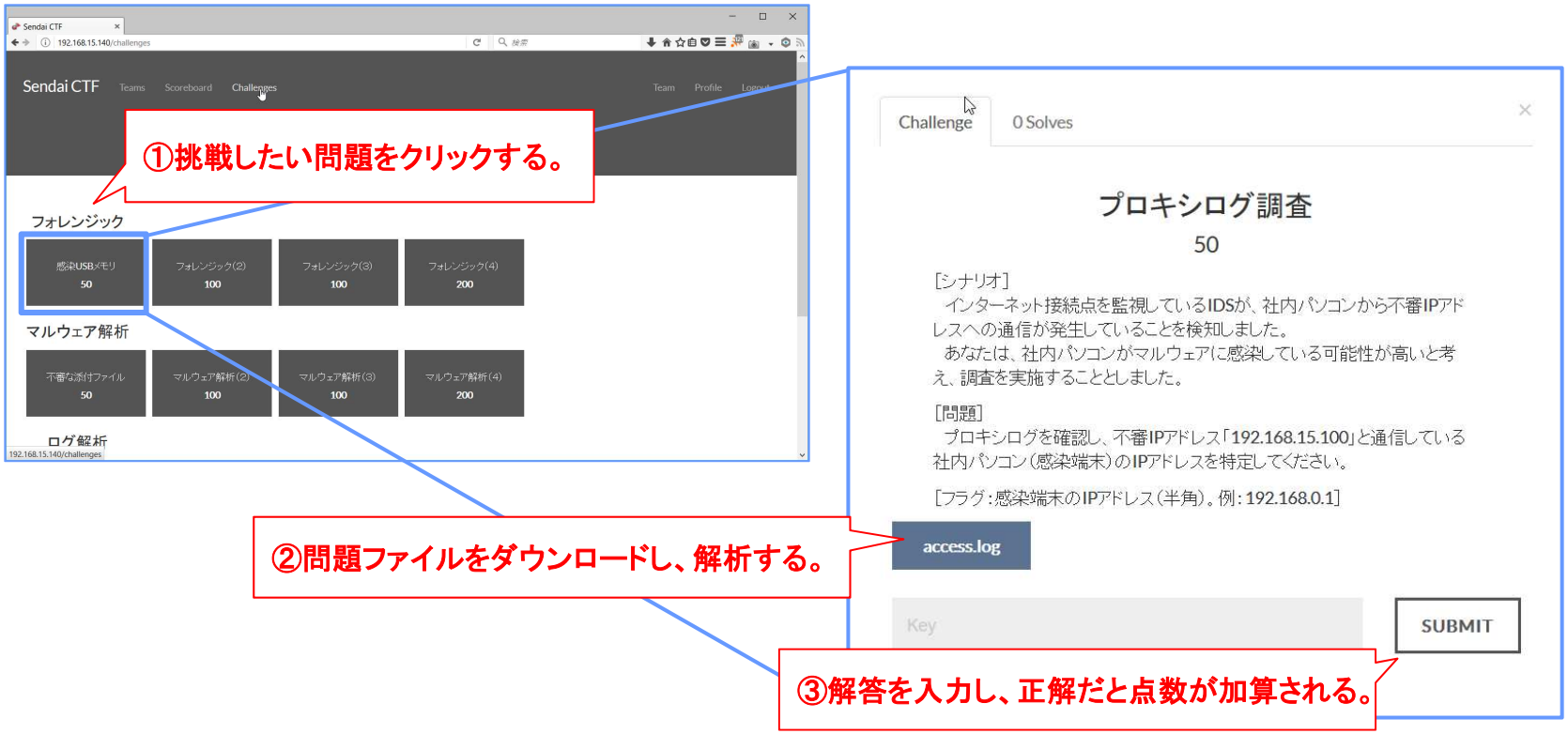
```
[ctfMacBook-Air:~ ctf$ log2timeline.py -V

plaso - log2timeline version 1.5.1

[ctfMacBook-Air:~ ctf$
```

動作確認済環境：Mac OS X 10.12.6

3.セキュリティ技術競技会（CTF）の概要と事前準備

セキュリティ技術競技会（CTF）の概要

- 参加者は、会場内に設置されたCTFスコアサーバにブラウザでアクセスし、登録されている問題に挑戦します。
- 解答をCTFスコアサーバに入力し、正解すると点数を獲得します。
- 競技時間内に獲得した点数により、順位を決定します。



競技ルール

順位判定

- 個人戦で、競技時間内に獲得した点数を競います。
- 同点の場合、その点数に早く到達した人が上位となります。

禁止事項

- CTFスコアサーバに不正アクセスまたは過度な負荷をかけるなど、運営を妨害する行為
- 他の参加者の競技を妨害する行為
- 他の参加者に問題の解法等を教える、または教えてもらう行為
- その他、運営事務局が不適切と判断し注意した事項を繰り返す行為

※禁止事項を発見した場合は、運営事務局の判断により失格とし、退場していただく場合があります。

仙台CTFの特徴

- **ログ解析、マルウェア解析、フォレンジック、セキュリティ診断など、さまざまなジャンルの問題が出題されます。**
- **各ジャンルごとに「株式会社仙台シーテーエフ」で発生したシナリオが設定されており、問題を順番に解いていくことで、シナリオを楽しむことができます。**

（補足）問題は難易度順に登録されているとは限らないため、解けそうな問題から挑戦しても構いません。

◆ **出題ジャンル「ログ解析」のシナリオと問題のイメージ**

<u>シナリオ</u>
昨日の夜中、DMZに設置しているウェブサーバのレスポンスが低下しました。どうやら大量アクセスにより、負荷が高くなっていたようです。あなたは、ウェブサーバのログを確認することとしました。

問題1 （100点）
ウェブサーバのアクセスログを分析し、大量アクセスをしていたIPアドレスを特定してください。

問題2 （50点）
実は大量アクセスをしていたIPアドレスは□□□でした。□□□を調査して□□□の原因を特定してください。

問題3（100点）
調査により、□□□であることが判明しました。追加調査により、□□□を特定してください。

問題4（200点）
当面の対策として、□□□を検討することとなりました。□□□を分析してください。

出題ジャンルとシナリオ

出題ジャンル	シナリオ
復習問題	• インターネット接続点を監視しているIDSが、社内パソコンから不審IPアドレスへの通信が発生していることを検知しました。あなたは、社内パソコンがマルウェアに感染している可能性が高いと考え、調査を実施することとしました。
ログ解析	• 昨日の夜中、DMZに設置しているウェブサーバのレスポンスが低下しました。どうやら大量アクセスにより、負荷が高くなっていたようです。あなたは、ウェブサーバのログを調査することとしました。
マルウェア解析	• 最近、毎日のように、複数の社員から、不審メールが届いたとの通報があります。毎回、受信者ごとにメールの差出人、件名、本文などはランダムに設定されています。添付ファイル名もランダムに設定されていますが、受信日が同じであれば、ファイルの内容（ハッシュ値）は同じであり、開封すると不審な通信が発生します。さて、本日も不審メールが届いたとの通報がありました。あなたは、添付ファイルを解析し、不審通信先を確認することとしました。
フォレンジック	• 工場用PCで利用しているUSBメモリからマルウェアが検出されました。どうやら工場用PCがマルウェアに感染してしまったようです。あなたは、工場用PCが感染した原因を調査することとしました。
セキュリティ診断	• 営業部門では、インターネットを通じて不特定多数からアクセスされる顧客向けウェブサービスの開発を進めています。あなたは、営業部門から相談を受け、セキュリティに問題がないか点検することとしました。
雑学	• 情報セキュリティ関する知識を問うクイズ問題です。（シナリオはありません）

セキュリティ技術競技会（CTF）の事前準備

- 各自がCTFに必要と考えるツールをご準備ください。
- 必要なツールを予想し、準備することもCTFの競技の一部です。

- なお、別途、練習問題を公開する予定です。詳細は、仙台CTF公式ウェブサイトでお知らせいたします。

仙台CTF公式ウェブサイト
http://sectanlab.sakura.ne.jp/sendaictf/