仙台CTF 2018 説明書
（一般公開版）

2018年11月

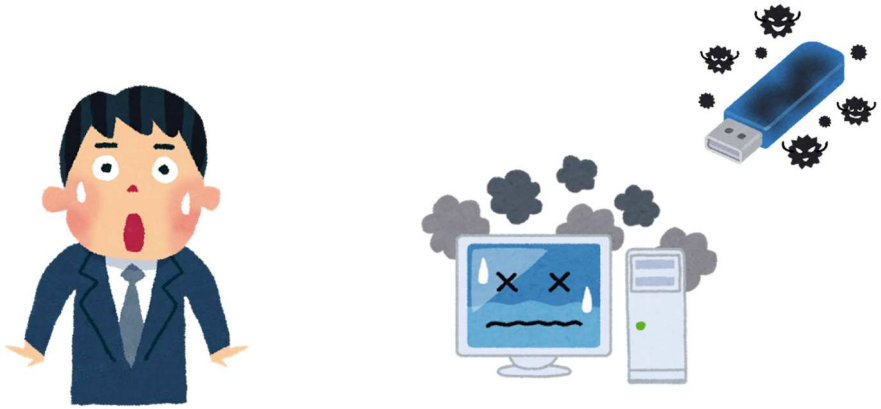
仙台CTF推進プロジェクト

目次

1.仙台CTFの舞台設定と競技ルール

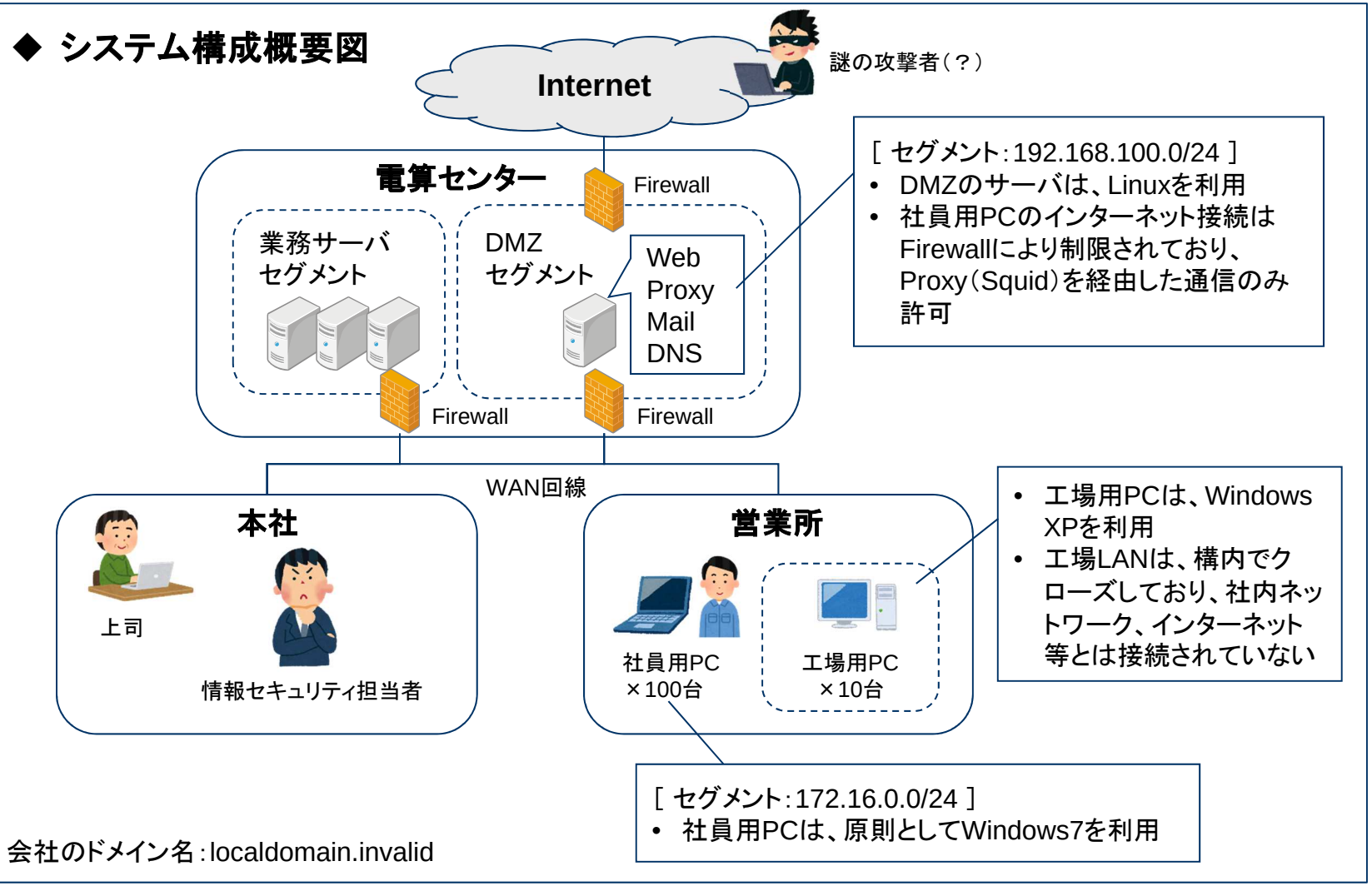
仙台CTFの舞台設定

- 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



仙台CTFの特徴

- **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「復習問題」のシナリオと問題のイメージ

シナリオ

ある日、営業所の社員用パソコンのウイルス対策ソフトから、ウイルス検知アラートが通知されました。

社員に電話連絡し状況を確認したところ、しばらく利用していなかった社員用パソコンを久しぶりに起動し、最新パターンファイルに更新のうえ手動でオンデマンドスキャンを実行したところ、デスクトップに作成されていた身に覚えのないファイルを、マルウェアとして検知したようです。

あなたは、検知したファイル（検体）は、過去のいつかの時点で感染していたマルウェアである可能性が高いと判断し、社員用パソコンから調査に必要となるエビデンスを証拠保全のうえ、感染原因を調査することとしました。

問題1 （100点）
検体が作成および起動された日時を特定してください。

問題2 （100点）
あなたは、感染パソコンをタイムライン解析したところ、ウェブサイト閲覧中に脆弱性攻撃を受けた痕跡を発見しました。
$MFTのタイムライン解析、ならびにIEの一時ファイルの解析により、感染に利用された脆弱性攻撃コードのファイル名を推測してください。

問題3（100点）
あなたは、脆弱性攻撃コードのダウンロード元URLを特定し、プロキシサーバで通信を遮断したいと考えました。
Internet Explorerの一時ファイルを解析し、脆弱性攻撃コードのダウンロード元URLを特定してください。

出題ジャンルとシナリオ

出題ジャンル	説明
復習問題	• Day-1セキュリティ技術勉強会の実習と同様の手順で回答できる問題です。
マルウェア解析	• 動的解析や静的解析により、マルウェアが通信するIPアドレスなどの挙動を特定する問題です。
フォレンジック	• マルウェアに感染したパソコンのディスクイメージ、レジストリ、メモリなどを解析し、いつ、何が起きたのか特定する問題です。
セキュリティ診断 【非公開】	• 診断ツールなどを利用し、ウェブアプリケーションやクライアントアプリケーションなどに存在している脆弱性を特定する問題です。
ネットワーク	• ネットワークパケット（PCAP）を解析し、トラブルの原因などを特定する問題です。
制御/IoT 【非公開】	• 制御システムのプロトコルや脆弱性に関する問題です。
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。

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

補足事項

- ブログ等で問題の回答方法（いわゆるwriteup）を掲載しても構いません。

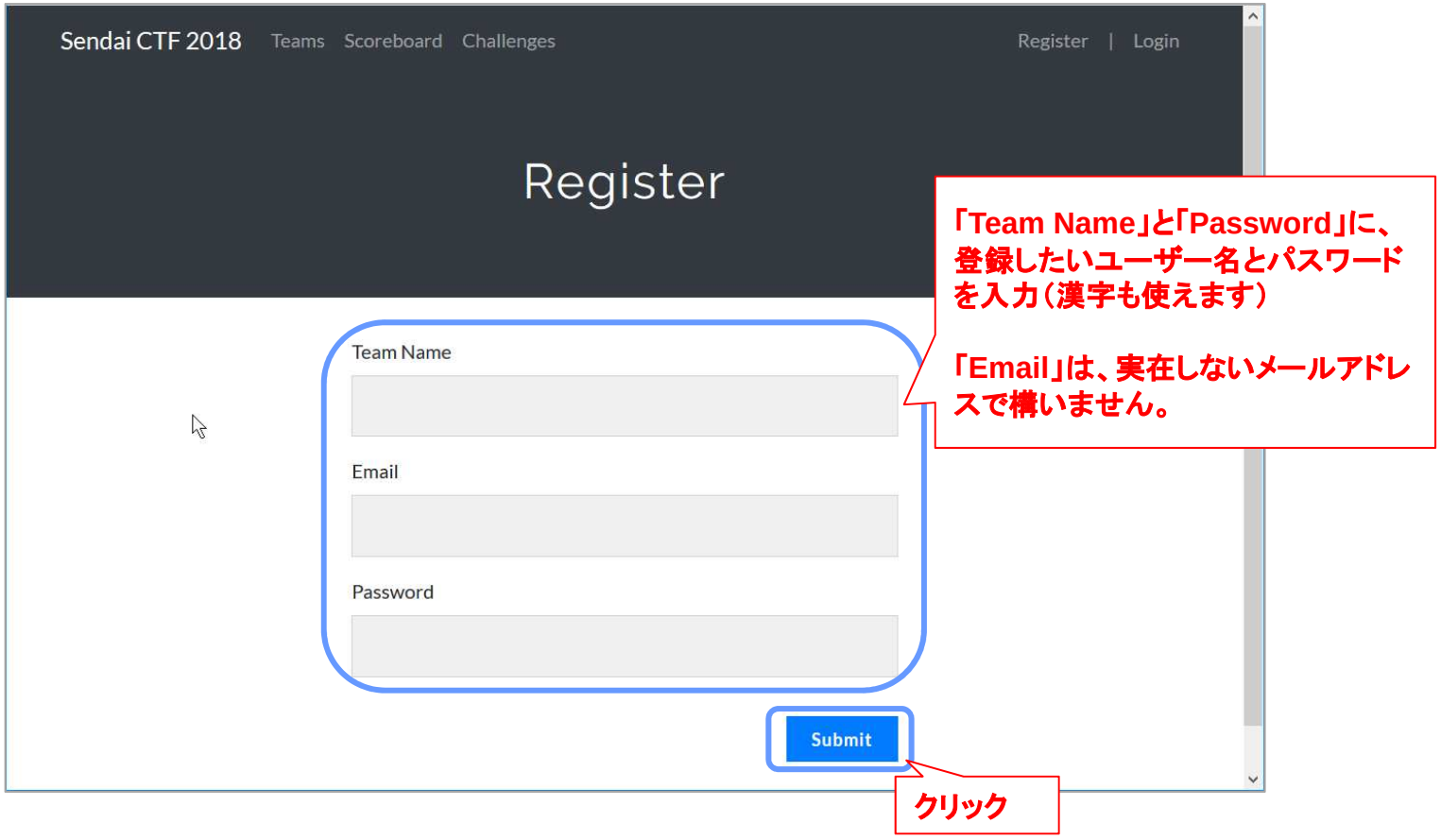
2.ユーザー登録

ユーザー登録（1）

① ブラウザで、「http://ctf.sectanlab.jp/」にアクセスします。
② 画面右上の「Register」をクリックします。

ユーザー登録(2)

③「Team Name」、「Email」、「Password」を入力し、「Submit」をクリックします。



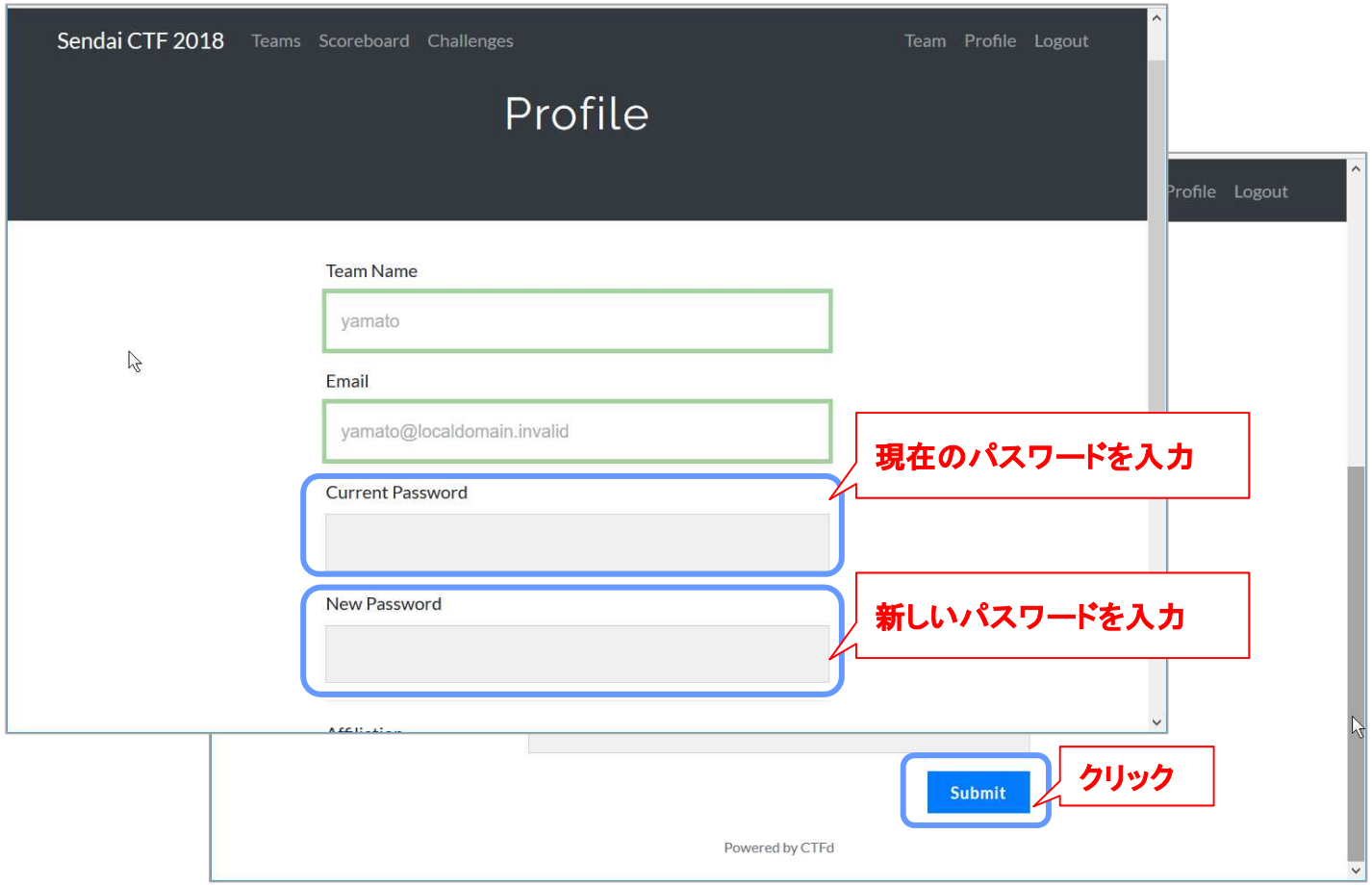
（参考）パスワード変更方法（1）

① 画面右上の「Profile」をクリックします。

（参考）パスワード変更方法（2）

② 「Current Password」欄に現在のパスワードを入力、「New Password」欄に、新しいパスワードを入力し、画面最下部にある「Submit」をクリックします。

以上の操作で、初期パスワードの変更は完了です。

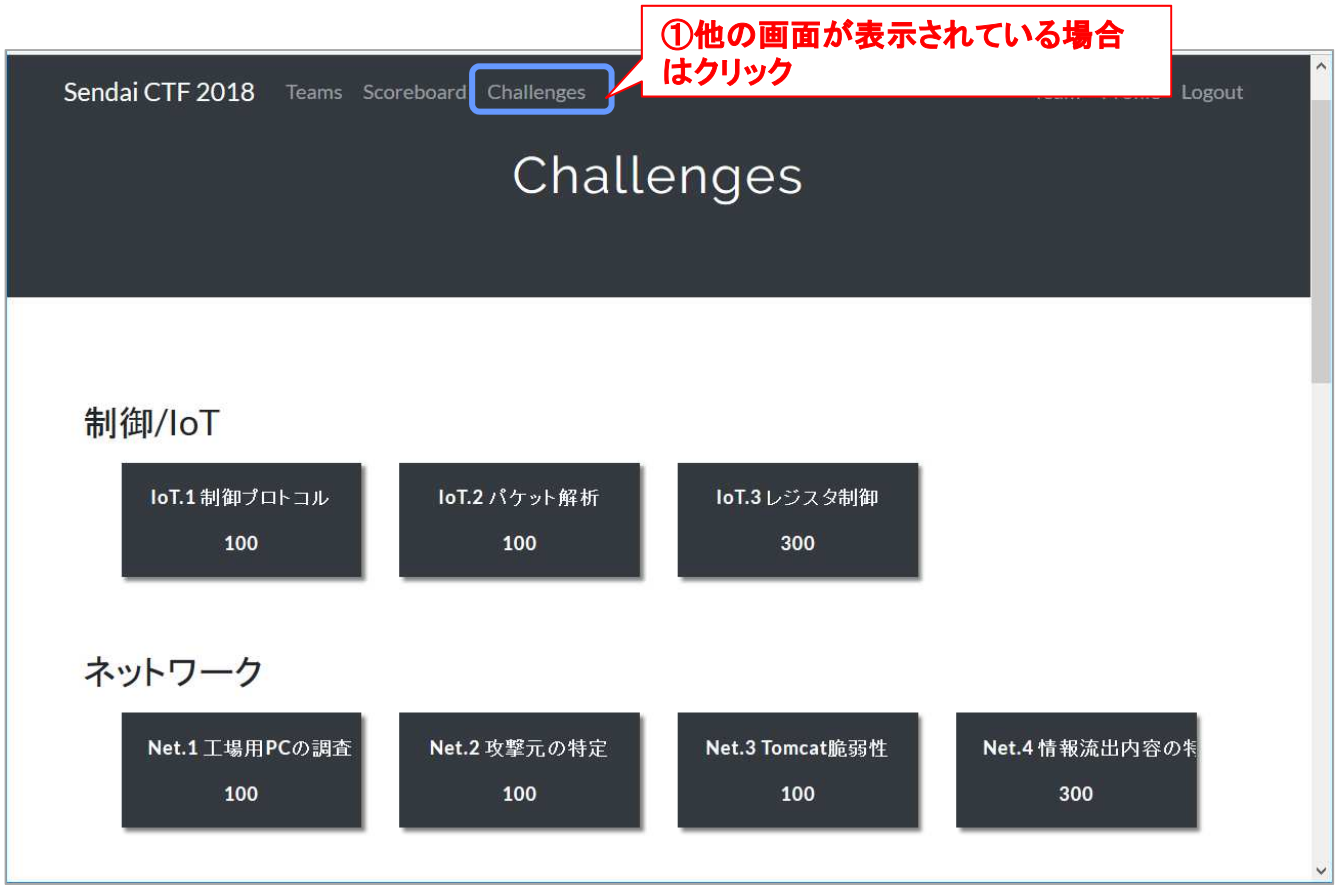


3. 問題の確認と回答

問題の確認と回答（1）

① CTFスコアサーバにログインすると、「Challenges」画面が表示されます。

（他の画面が表示されている場合は、画面上部の「Challenges」をクリックします。）



問題の確認と回答（2）

② 挑戦したい問題をクリックし、問題の説明画面を表示します。

③ 問題の内容を熟読のうえ、添付ファイル※1をダウンロードして解析するなど、指定された作業を行い、問題の答え（フラグ）を探し出します。 （※1　添付ファイルがない問題もあります。）

④ 探し出したフラグを、問題の説明画面にある「Flag」欄に入力し、「Submit」をクリックします。正解すると点数が加算されます。