# 仙台CTF説明書

2017年11月19日

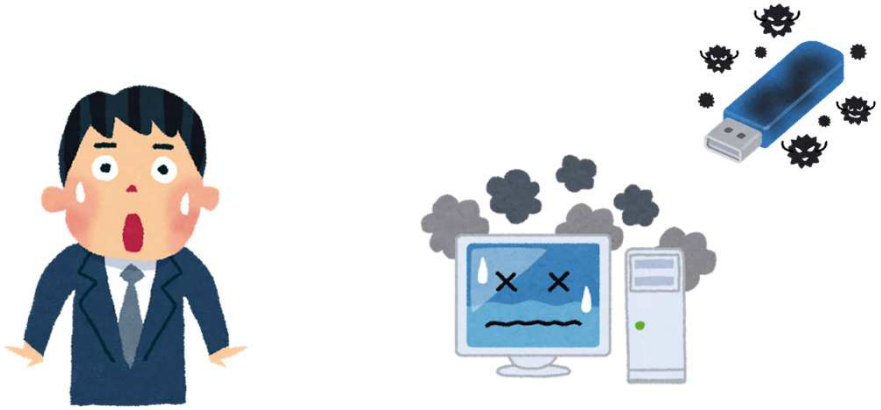
仙台CTF実行委員会

# 目次

# 1.仙台CTFの舞台設定と競技ルール

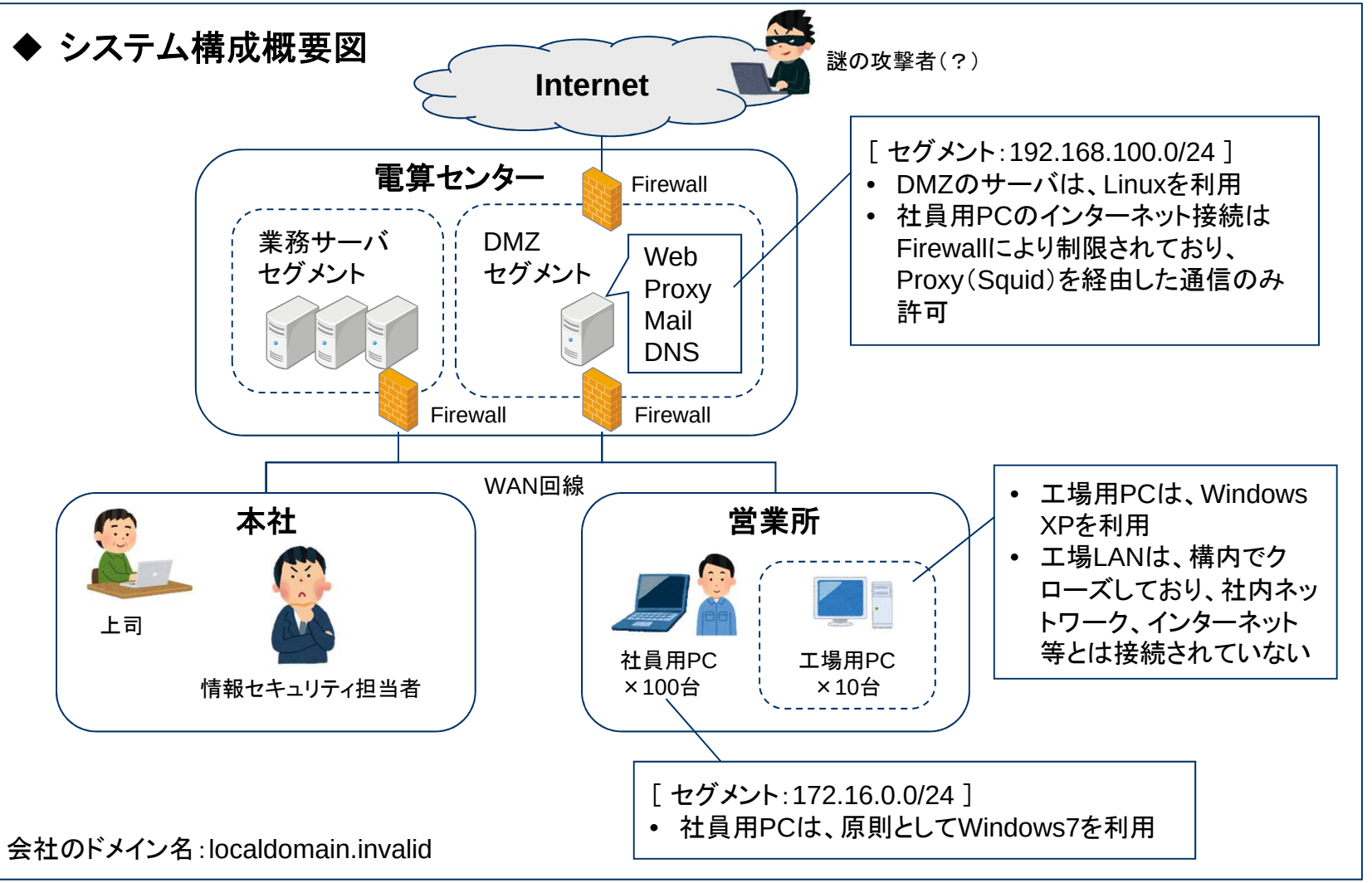
# 仙台CTFの舞台設定

- 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

- **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 （100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【非公開】 | • 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） |

# 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。

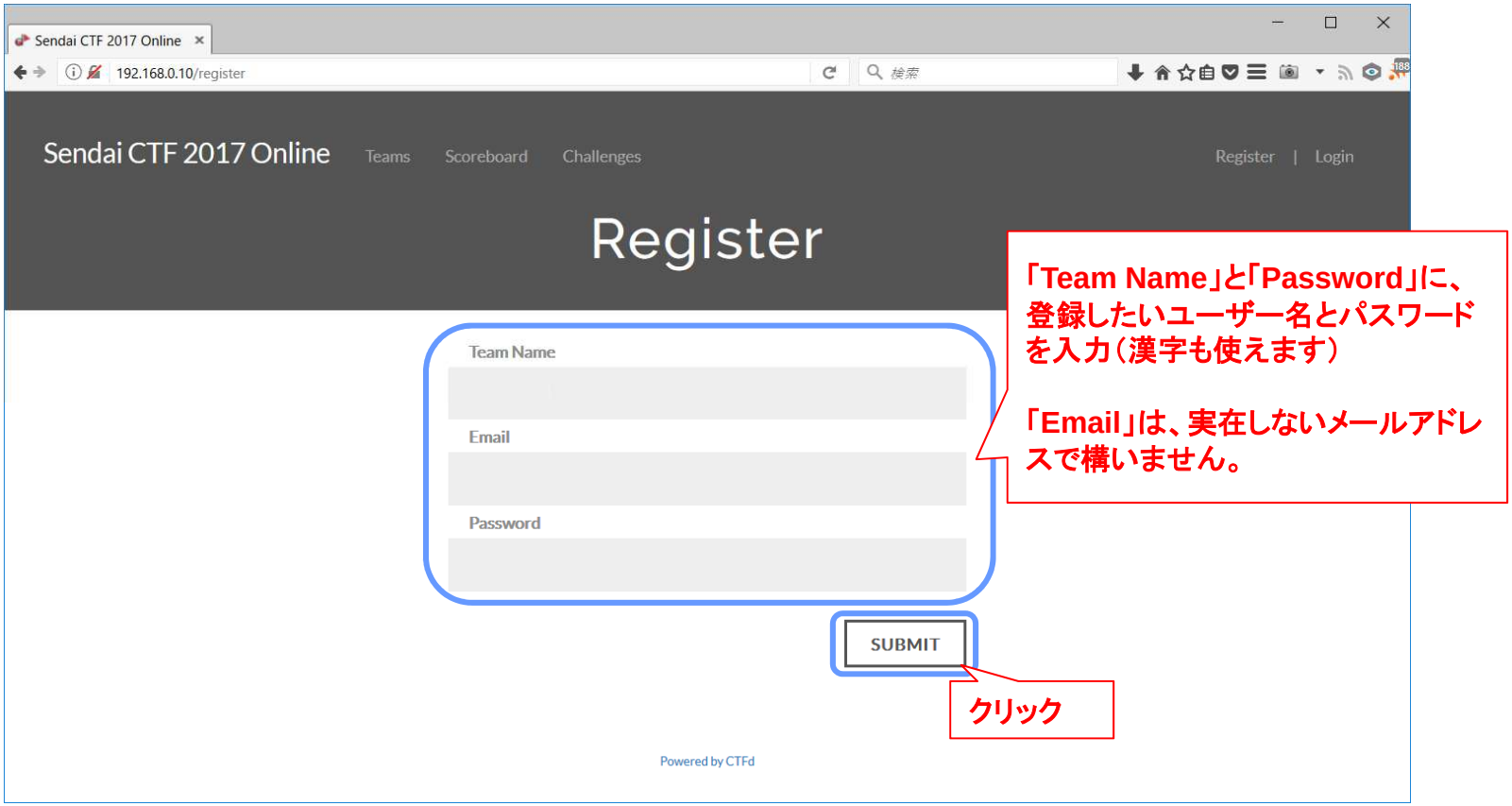
# 2.ユーザー登録

# ユーザー登録（1）

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

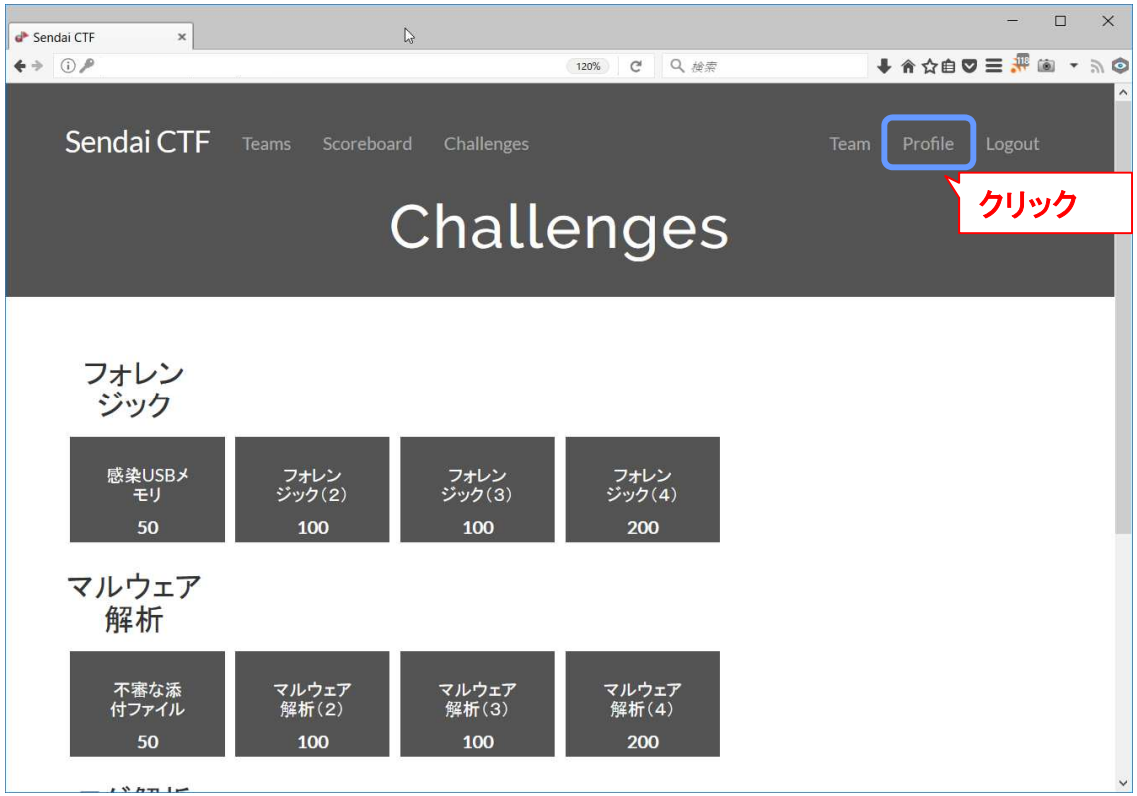
# ユーザー登録（2）

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）

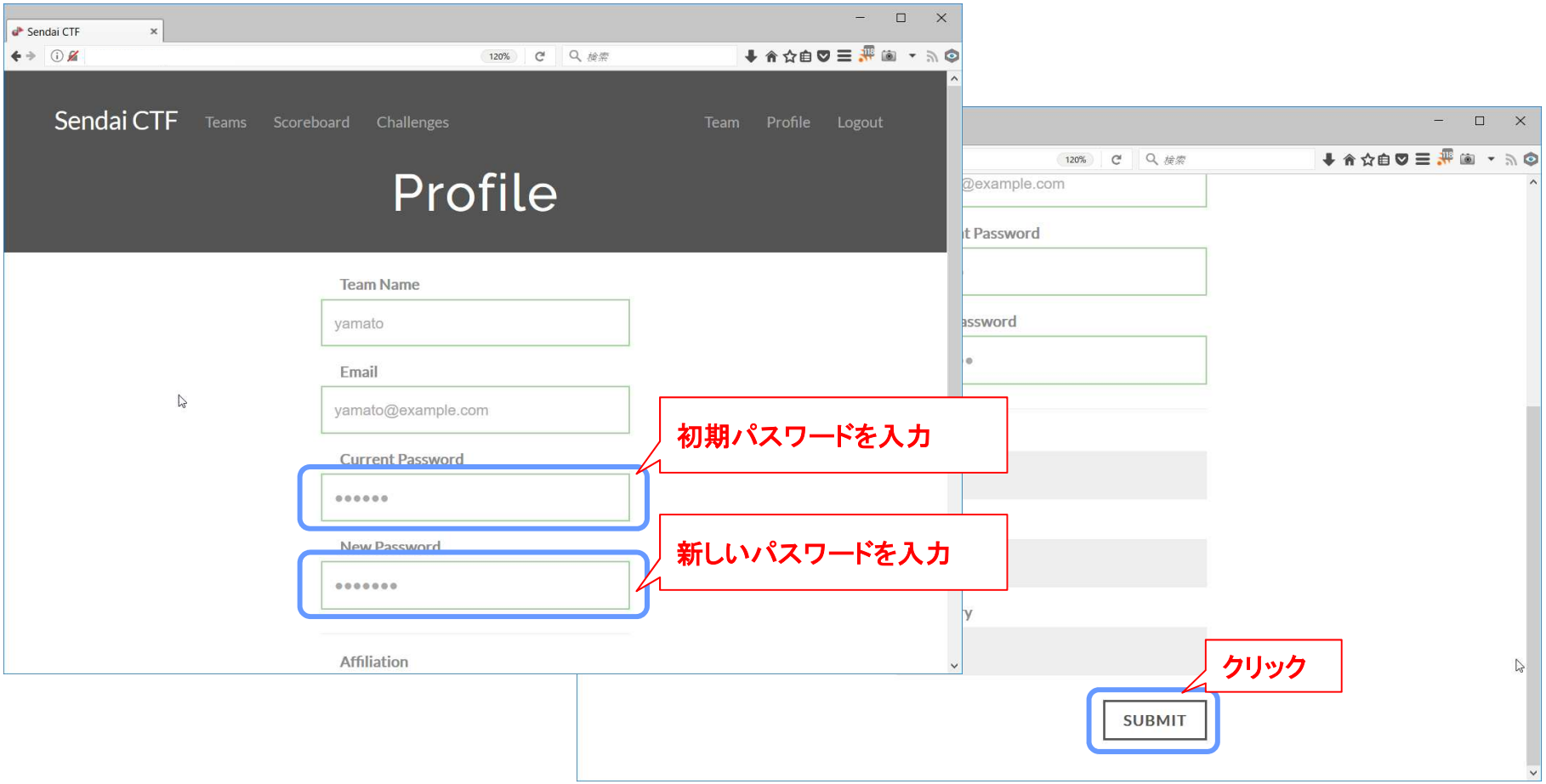
① 画面右上の「Profile」をクリックします。



# （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「Key」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。