**※第1章（SSL）、第4章（DNS）、第5章（Mailサーバー1）、第9章（UFW）ができていることが前提。  
DNSの設定変更が必要かもしれません**

**●実習１１－１．事前設定（UFWの設定）**

**UFW(ファイアウォール)でPrometheusが使用するポート番号を許可する**

（１）Prometheusで使用するポート（TCP:9090）と許可する。

①　指定されたポートを許可する。

**コマンド→　sudo ufw allow 9090/tcp**

➁　UFWの状態を確認する。

**コマンド→　sudo systemctl status ufw**

**●実習１１－２．Prometheusのインストール（Prometheus、node-exporter）**

監視ツールのPrometheusと監視対象に設定するnode-exporterをインストールする。

今回は、監視サーバーと監視対象は同じサーバーとする。

（１） Prometheus、node-exporterのインストール。

　 ① Prometheus、node-exporterをインストールする。

**コマンド→****sudo apt -y install prometheus prometheus-node-exporter**

（２） Prometheusの設定ファイルの確認・有効化

　 ① 設定ファイル（/etc/prometheus/prometheus.yml）を確認する。

**コマンド→****sudo vi /etc/prometheus/prometheus.yml**

➁ Prometheus、node-exportを有効化する。

**コマンド→****sudo systemctl enable prometheus prometheus-node-exporter**

③ 次のURLでPrometheusが動作のダッシュボードを確認する。

**http://IPアドレス:9090**

**グラフィカル ユーザー インターフェイス, アプリケーション

自動的に生成された説明**

**●実習１１－３．リソースの監視**

**上記のダッシュボードから、リソースの監視を行う。**

（１）調査可能なリソースの情報を収集し、グラフにして可視化する。

　①　次にあげるリソースについて、情報を収集して可視化する。

**＊監視するリソース・・・CPU、メモリ、ネットワーク（選択する項目は任意）**

選択したリソースの項目を各リソースひとつずつ記載する。

　　　　<例>CPU：node\_cpu\_seconds\_total

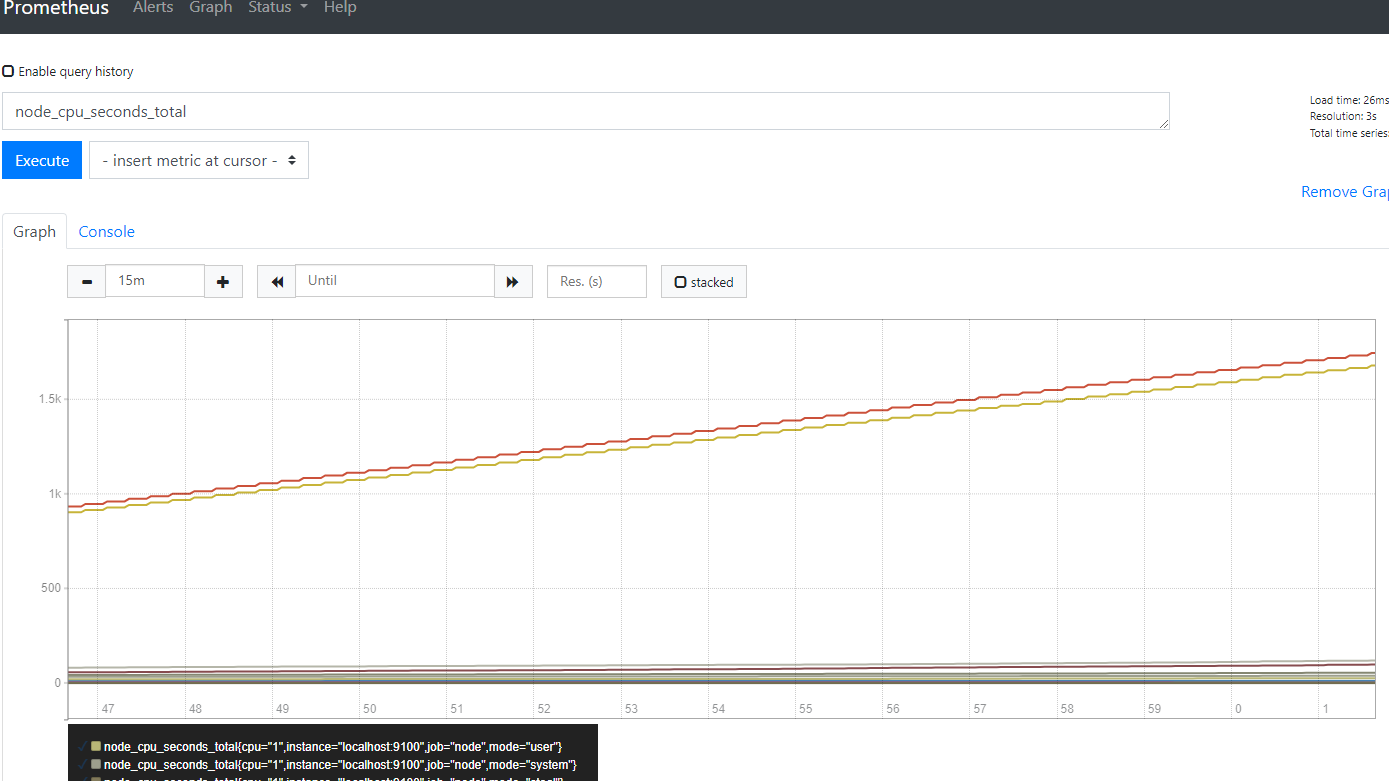
　　　CPU:[ node\_cpu\_seconds\_total ]

　　　メモリ:[ node\_memory\_Active\_anon\_bytes ]

　　　ネットワーク:[ node\_network\_info ]

②　表示したグラフのスクリーンショットを取り、クラス名番号名前prometheus-graph.jpgで保

存する。（1枚でOK）

****

**●実習１１－４．セキュリティ（HTTPSと認証）**

**Prometheusのダッシュボードにアクセスする時にHTTPS、Basic認証を行えるようにする**

**＊HTTPSで使用する証明書は以前の課題で作成したものを使用する**

（１）Basic認証用のユーザー、パスワードを作成する

　①　bcrypt hashでパスワードを生成する。

ユーザーID：クラス名番号、パスワード：123qwe

**コマンド→　sudo htpasswd -nB SK2A03**

　　＊生成されたパスワードはいったんテキストファイルにコピーしておく。

②　作成済みの鍵と証明書を/etc/prometheusディレクトリにコピーする

**コマンド→****sudo cp /ca/server.pem /etc/prometheus/**

**sudo cp /ca/private/server.key /etc/prometheus/**

③　②で作成した鍵と証明書のオーナーとグループをprometheusに変更する。

**コマンド→****sudo chown prometheus:prometheus /etc/prometheus/server.pem****sudo chown prometheus:prometheus /etc/prometheus/server.key**

（２）　設定ファイルを作成と編集。

　①　/etc/prometheus/web.ymlファイルを開く（新規ファイル）。＊パスに注意すること

**コマンド→**

**sudo vi /etc/prometheus/web.yml**

②　①で開いたweb.ymlに次の項目を追加して保存する

|  |
| --- |
| tls\_server\_config:  cert\_file: server.pem　　　　　　　　　　　　　・・・　証明書  key\_file: server.key　　　　　　　　　　　　　　　・・・鍵  #ユーザ名とパスワードを指定する(htpasswdコマンドで作成したもの)  basic\_auth\_users:  クラス名番号: パスワード |

③　/etc/default/prometheusファイルにweb.ymlファイルのパスを指定する

**コマンド→****ARGS="--web.config.file=****/****etc/prometheus/web.yml“**

**修正する内容（５行目付近）**

**ARGS="--web.config.file=/etc/prometheus/web.yml“**

④　鍵、証明書、ユーザーID、パスワード（平文）を/etc/prometheus/prometheus.ymlに追加する

**コマンド→**

**追加する内容（- job\_name: "prometheus"フィールド内に追記）**

|  |
| --- |
| **scheme: https**  **tls\_config: 　　　　　　　　#証明書と鍵の指定**  **cert\_file: /etc/prometheus/server.pem**  **key\_file: /etc/prometheus/server.key**  **insecure\_skip\_verify: true　　　　 #自己証明書の場合はtrue**  **basic\_auth:**  **#ユーザID、パスワードの指定**  **username: 'クラス名番号’**  **password: '123qwe'** |

⑤　Prometheusを再起動する

**コマンド→****sudo systemctl restart prometheus**

（３）　HTTPSと認証を確認する

　①　ブラウザを開き、次のURLでPrometheusにアクセスする。

　　　　https://IPアドレス:9090

②認証が聞かれ、ユーザーID（クラス名番号）、パスワード（123qwe）でログインできる確認する

**[　成功　]**

**●実習１１－５．アラートの設定**

**Prometheusのアラートをメールで送信する**

**＊事前にメールサーバーの動作を確認する。また、DNSの設定各種も必要に応じて変更する**

**こと。**

（１）Alertmanagerをインストール、設定する

　①　Alertmanagerのインスール

**コマンド→****sudo apt -y install prometheus-alertmanager**

②　alertmanager.ymlファイルのバックアップと新規作成。

**コマンド→****sudo vi /etc/prometheus/alertmanager.yml**

設定

＊設定は配布されたalertmanager.ymlを編集すること。

　　　SMTPサーバー：localhost 送信元：root@ecccomp.ac.jp

受信者（receiver）：email-notice 送信先：クラス名番号@ecccomp.ac.jp

（２）　アラートルールの設定

　①　ルールの設定ファイルを新規作成（/etc/prometheus/alert\_rules.yml）

**コマンド→:** **sudo vi /etc/prometheus/****alert\_rules.yml**

②　ルールの内容を追加する。

CPUの使用率が平均20％を超えるか 監視する。＊alert\_rules.ymlファイルを使用する

③　アラートの対象とルールを指定する（/etc/prometheus/prometheus.yml）

**コマンド→****sudo vi /etc/prometheus/prometheus.yml**

Alertmanager (稼働ホスト)：localhost ポート番号：9093

ルールファイル：alert\_rules.yml

（３）　Prometheusの再起動、Alertmanagerの有効化

　①　Prometheus、Alertmanagerの再起動

**コマンド→:****sudo systemctl restart prometheus prometheus-alertmanager**

②　Alertmanagerの有効化

**コマンド→**

**sudo systemctl enable prometheus-alertmanager**

（４）　設定ファイルのコピー

　①　/etc/prometheus/prometheus.ymlをprometheus.kad11.ymlで保存する

**コマンド→** **sudo cp /etc/prometheus/****prometheus.yml Prometheus.kad11.yml**

（５）　アラートの確認

　①　ダッシュボードの「Status」>「Rules」で設定したルールが適用されているか確認する

　　　State：[　OK　・　ERROR　・　UNKNOWN]

　　＊適用されていれば「OK」と表示される。

②　CPUの負荷を上昇させるため、次のコマンドを複数回入力する

**コマンド→**

**yes > /dev/null &**

③　現在のCPUの状態をリアルタイムで確認する

**コマンド→**

top

④　アラートが発生したかダッシュボード（Alerts）で確認する

[ Firing]が検知されているか確認する

グラフィカル ユーザー インターフェイス, テキスト, アプリケーション, メール

自動的に生成された説明

**※アラートが発火しない場合は、コマンド入力回数や検出しきい値を調整する。**

　⑤　アラートメールを確認する

**コマンド→**

**telnet localhost 110**

＊ログイン　・・・　メール送信先のユーザーでログインする。

　　　Alertmanagerからのメールを確認後、確認したメールをコピー&ペーストしてalertmail.kad11.txt

で保存する。

**●チェック項目：以下をチェックします。**

* **実習１１－４（３）  
  ブラウザ（シークレットウインドウがいいかも）から<https://IPアドレス:9090> にアクセスして、ユーザ名：クラス番号、パスワード：123qweでログインできる**
* **実習１１－５（５）⑤  
  Alertmanagerからメールが来ていることを確認する**

**●実習１１－６．提出用ファイルの作成と提出**

①prometheus.kad11.yml、web.yml、alertmail.kad11.txtをコピー＆ペーストしてクラス名番prometheus.kad11.yml、クラス名番号web.yml、クラス名番号alertmail.kad11.txt保存する。

**●課題提出**

**４つのファイル（クラス名番号名前prometheus-graph.jpg、クラス名番号prometheus.kad11.yml、クラス名番号web.yml、クラス名番号alertmail.kad11.txt）とログファイル（クラス名番号日付.log）を、「実習11\_クラス番号氏名」のフォルダに入れて、sv23へ提出しなさい。**