令和 5 年度高エネルギー加速器研究機構技術研究会、2024 年 3 月 7～8 日
https://www2.kek.jp/engineer/tsukuba/giken/2023/

技術情報共有サイトの立ち上げ（Discourse のインストールと設定）

○内藤茂樹#
自然科学研究機構 分子科学研究所

概要

本年度分子科学研究所では、研究教育に関わる機関に所属する技術者に対して技術情報の共有・蓄積および交流の場を提供することを目的とする「技術情報共有サイト」を立ち上げた。本サイトは Rocky Linux9 上に Discourse を構築して運用しており、発表者が構築や保守等の作業を行っている。

今回の発表では Discourse のインストールと設定を中心に、Discourse から送信されるメールを Gmail の「メール送信者のガイドライン」に対応するため SPF、DIKM、DMARC、ARC に対応したことや、SELinux の問題により Discourse が立ち上がらなくなったことへの対処等を報告する。

1. 技術情報共有サイトについて

研究・教育機関に所属する技術者に対して、技術情報の共有・蓄積および交流する場を設けることで研究教育現場における技術サービスを向上させることを目的に開設した、掲示板を主体とするサイトである。また参加資格は以下のとおりである。

- 以下のいずれかに該当する機関に雇用されているもの及び雇用されていたもの
  - 国立・公立・私立大学法人（高等専門学校を含む）
  - 国立・公立研究機関（独立行政法人を含む）
- 上記に該当する機関が開催した技術研究会で発表したことがあるもの
- 本サイトの目的に賛同し、利用規約を遵守するもの
- 運用者が特に認めたもの

参加方法は招待制を採用しているので、参加希望者は既に登録済みのユーザもしくは管理スタッフに問い合わせていただくことになる。

2. Discourse

本サイトは、Rocky Linux9 上に構築した Discourse にて運用している。なお Rocky Linux は Red Hat Enterprise Linux 互換の OS である。

2.1 Discourse とは

Discourse はオープンソースのコミュニケーションプラットホームである。メインとなる提供サービスは掲示板であり、チャット機能も搭載している。ユーザはグループ分けが可能なので、目的別や分野別に纏まることがでる。またセキュリティにも配慮されており、Google や Microsoft 等の Authenticator を使う二要素認証が設定できる。詳しくは公式ウェブサイト（https://www.discourse.org/）を参照してほしい。

2.2 Discourse のインストール

Discourse はコンテナ仮想化である docker 上で動くため、まず docker をインストールする。docker のインストールには docker の公式レポジトリを追加することが必要である。レポジトリ及び docker 本体とも dnf コマンドでインストールできる。docker のインストールが終わったら起動しておく。

続いて Discourse をインストールする。Discourse のインストールは dnf コマンドではできない。git からソースファイルをダウンロードし、インストーラースクリプトを実行する。インストールが完了すると自動的に起動する。

Discourse にユーザを追加するときに、そのユーザ宛てにメールが送信されるため、ホスト OS（本サイトでは Rocky Linux9）上に SMTP サーバを構築する。本サイトでは Postfix を構築した。

Discourse の設定は WebUI 上で行うため、ブラウザで Discourse にアクセスする。管理用ユーザである admin の初期パスワードは最初のログイン後に変更しておく。その後管理者となるユーザを別途登録し、管理者ロールを付けておく。以後は admin では無く管理者ロールを付けたユーザで設定変更等の作業を行う。

3. Gmail の「メール送信者のガイドライン」への対応

2024 年 2 月以降に Google Workspace を除く Gmail 宛てにメールを送る場合のガイドラインが Google より出された。特に 1 日 5,000 件以上出している場合は厳しく、SPF 及び DKIM の両認証と DMARC の設定、さらにメーリングリストを運用している場合は ARC 認証も必要となった。このうち SPF は送信元ドメインを IP アドレス等で認証するもので、設定自体は DNS サーバに SPF 用の TXT レコードを設定するだけでよく、サーバ自体に変更を加える必要は無い。メールを送信するだけなら DMARC も原則同じである。しかし他の 2 つについては、別途ソフトウェアを導入する必要がある。本サイトではメールを受信した時のことを考慮して Postfix が DMARC に対応するためのソフトを導入した。また Discourse が送信するメールは docker 上からホスト OS 上の SMTP サーバを経由することから ARC にも対応する事にした。

3.1 DKIM への対応

DKIM はサーバ上でメールに電子署名を施す事によって送信元ドメインを認証するものである。その

snaito@ims.ac.jp

ため電子署名を行うソフトウェアをサーバにインストールする必要がある。本サイトでは opendkim を使用することとした。

opendkim のインストールには crb レポジトリが enable である必要がある。まず crb レポジトリを enable にして、dnf コマンドで opendkim をインストールする。

インストール後、初めに電子署名に必要な秘密鍵と公開鍵のペアを作成する。作成した秘密鍵を“/etc/opndkim/keytable”ファイルに登録する。公開鍵は DNS の TXT レコードを用いて配布するので、このファイルに登録する必要は無い。続いて“/etc/opendkim/SignningTable”に From 行に使うドメインと秘密鍵の組み合わせを記述する。最後に“/etc/opendkim.conf”ファイルで opendkim 自体の設定を行う。

3.2 DMARC への対応

DMARC は SPF や DKIM の認証に失敗した時にどのような動作を求めるかを定めるものである。定めた内容は DNS の TXT レコードを利用して配布するのでメールを送信するだけの場合は追加のソフトウェアを必要としない。しかし本サイトでは受信する場合も考慮して opendmarc をインストールした。インストール自体は dnf コマンドを使用し、設定は“/etc/opendmarc.conf”で行う。本サイトではデフォルトのままで特に変更はしていない。

3.3 ARC への対応

ARC はメーリングリストサーバのような中継サーバが付ける Received 行の認証を行うものである。認証は DKIM と同じく電子署名を施す方法なため、別途電子署名を行うソフトウェアが必要である。本サイトでは openarc を使用することとした。

openarc のインストールは dnf コマンドで行う。

本サイトでは、電子署名に使う公開鍵と秘密鍵のペアは DKIM のものを流用した。ただしオーナーとグループを opemarc のものにする必要があるため、DKIM の秘密鍵を“/etc/openarc”ディレクトリにコピーして、ファイルのオーナーとグループを openarc に変更した。openarc の設定は“/etc/openarc.conf”で行う。基本的に設定する項目は秘密鍵に関するものなので、opendkim と同様に設定する。公開鍵の配布も DKIM 同様に DNS の TXT レコードを使用するが、本サイトでは鍵ペアを DKIM のものを流用したため TXT レコードも DKIM のものを流用して、ARC 用の TXT レコードの新設はしていない。

3.4 DNS の TXT レコードの設定

SPF、DKIM 及び DMARC は DNS の TXT レコードに必要事項を記述して、受信サーバが情報を取得できるようにしておく必要がある。

SPF は送信するメールの From 行に使うドメインの TXT レコードとして、サーバの IP アドレス等やアクションを記述する。DKIM は専用のサブドメインを用いる。opendkim の場合、鍵ペアを作成したときに TXT レコードに記述する内容が書かれたテキストファイルが生成されるので、その内容を記載すれば良い。

DMARC はメールの From 行に使うドメインに“_dmarc.”というサブドメインを専用に用いる。このサブドメインの TXT レコードにアクションと、受信サーバから送られてくるレポートを受け取るメールアドレスを記載する。

3.5 Postfix の設定変更

本サイトでは SMTP サーバとして Postfix を使用している。Postfix と opendkim、opendmarc 及び openarc との連携は各 UNIX socket を使う。そのため sock ファイルに Postfix がアクセスできる必要があることから、Postfix のセカンダリグループとして opendkim、opendmarc 及び openarc を登録した。

また、Postfix 自体の設定として“/etc/postfix/main.cf”ファイル中に“non-smtpd_milters”と“smtpd_milters”に対して各 sock ファイルを設定した。

最後に Postfix を再起動して設定の変更を有効化した。

3.6 テストメールの送信とヘッダーの確認

Postfix が起動したら実際にテストメールを出して確認する。テストメールは Discourse の管理者メニューのメールタブから送信出来る。

図 1. テストメールの送信

テストメールを送信すると「[技術情報共有サイト]メール配信可能性テスト」という題名のメールが届く。そのメールのヘッダーを表示して、“Authentication-Results”ヘッダーで dkim、arc、spf、dmarc が「pass」となっている事を確認した。ヘッダーの確認の際に、Discourse は docker 上で動作していることから、最初は docker(172.17.0.2 等)からの送信情報が記録されている。確認するのは相手先の SMTP サーバが付けた“Authentication-Results”ヘッダーであることに注意する必要がある。

4. SELinux に引き起こされた問題

本サイトを立ち上げる前にテスト用として構築した別の Discourse サイトが起動しなくなる現象が発生した。本サイトでも発生する可能性があるため調査したところ、SELinux により拒否されているようだった。ただしモードは“Permissive”であり、本来ならログを記録するのみで制御は行わないはずである。あらためて SELinux 自体について調べたところ、RedHat のサイトに「Permissive モードで SELinux を実行すると、ユーザやプロセスにより、さまざまなファイルシステムオブジェクトのラベルが間違って設定される可能性があります。」との記述があった。こ

れはモードを“disable”から“permissive”に変更したときの注意書である。同じ箇所に“fixfiles -F onboot”実行して“/.autorekabek”ファイルを作成し再起動をすると直るとの記述があったので実行したところ、Discourse が起動したことが確認できた。

5. まとめ

技術情報共有サイトを立ち上げたいとの話を受けて、Rocky Linux9 に Discourse をインストールした。インストール自体は提供されるスクリプトを実行すれば良く、ソースからの make は不要であり比較的簡単な部類に入ると思われる。

また Google より Gmail にメール送信するときのガイドラインが出され、その対応に迫られた。ただこちらも各ソフトウェアは dnf コマンドにてインストール可能であり、設定もドキュメント通り行えば良く、比較簡単な部類に入ると思われる。ただし、DNS サーバ上に TXT レコードの登録が必要であり、サーバ単体で完結しないのが難点である。

本サイトとは別のサーバで Discourse が立ち上がらなくなるという障害が発生した。調べたところ SELinux により引き起こされたものと判った。モードが“permissive”でもサービスが起動しなくなる可能性があることが判った。

6. 技術情報共有サイトの紹介

報告の最後に技術情報共有サイトの紹介を行わせていただく。本サイトで主となるサービスはトピックと表記されるいわゆる掲示板である。各トピックは関連性の高いものを集めたカテゴリで分類することができる。カテゴリはサブカテゴリでさらに分類できる。自分の興味のある分野をカテゴリやサブカテゴリで見つけ、その中から読みたいトピックを見つけることになる。勿論検索もできるので、キーワードが判っていればトピックを見つけることは容易である。目的のトピックが見つかったら閲覧してみよう。そして是非トピックに参加してもらいたい。

本サイトは大学や共同利用機関の技術者を主に対象としているため、各専門分野に特化した情報の交換が可能である。インターネットで検索しても出てこない専門分野に特化した情報に関して、本サイトでは先達者がトピックを書いている可能性があるし、先達者を探し出すことができるかもしれない。

本報告書を読んで技術情報共有サイトに御興味を持っていただけたら幸いである。是非本サイトにアクセスして参加をしていただければと思う。図 2 は本サイトにアクセスしたときに最初に表示される画面である。公開してあるトピックはそのままゲストとして閲覧できるし、ユーザ登録してあれば右上のログインボタンからログインして限定公開のトピックに参加することができる。本サイトにユーザ登録を希望される場合は、左メニューの“ユーザー”を選択すると登録されているユーザ一覧が表示されるので、知り合いの方がいればその方に招待をお願いして欲しい。知り合いがいない場合は、左メニューにある“サイト情報”に書かれた「お問い合わせ」にある管理スタッフの連絡先にユーザの登録希望を知らせていただきたい。

最後に本サイトの URL を記載しておく。

URL ： https://tech-share.ims.ac.jp/

図 2. 技術情報共有サイト