API使用者驗證 & 授權

事前準備：建立帳號

> *先確保模擬 DB INTRA 的資料庫（data-intra.sql）內有沒有自己的部門、員工資料*

data-intra.sql

```
--  DB_INTRA

--
INSERT INTO DEPTB (DPT_CD,DPT_NAME,UP_DPT_CD,DPT_HEAD) VALUES('VL908', ' ', NULL, '911384');

-- ( )
INSERT INTO ViewMail2_IMG (EMP_NO,USR_ID,EMP_NAME,EMAIL,DPT_CD,MGR_ID) VALUES('911384', 'B1384', '',
'test@fubon.com', 'VL908', null);
```

> *在myTest專案的主要資料庫（data-primary.sql）建立登入者帳號資料*

data-pimary.sql

```
-- ( )
INSERT INTO MYTEST_ACCOUNT (ID, ENABLED, EMPLOYEE_ID) VALUES ('1', '1', '911384');
```

使用者驗證 Authentication

啟用方式

```java
@ComponentScan(basePackages = {"com.fubonlife.mytest.common", "com.fubonlife.mytest.api"})
@EnableFblDataBind
@EnableFblAsync
@EnableFblSwagger(basePackages = "com.fubonlife.mytest.api.controller")
@EnableFblCrowd
@EnableFblJwt
@EnableFblCors
@EnableFblSecurity
@EnableFblErrorHandle
@EnableFblPia
@EnableFblRequestLogging
@SpringBootApplication
@Slf4j
public class Application extends SpringBootServletInitializer {

    @Override
    protected SpringApplicationBuilder configure(SpringApplicationBuilder application) {...}

    public static void main(String[] args) {
        TimeZone.setDefault(TimeZone.getTimeZone("Asia/Taipei"));
        DateTimeZone.setDefault(DateTimeZone.forTimeZone(TimeZone.getDefault()));
        ApplicationContext ctx = SpringApplication.run(Application.class, args);
    }
}
```

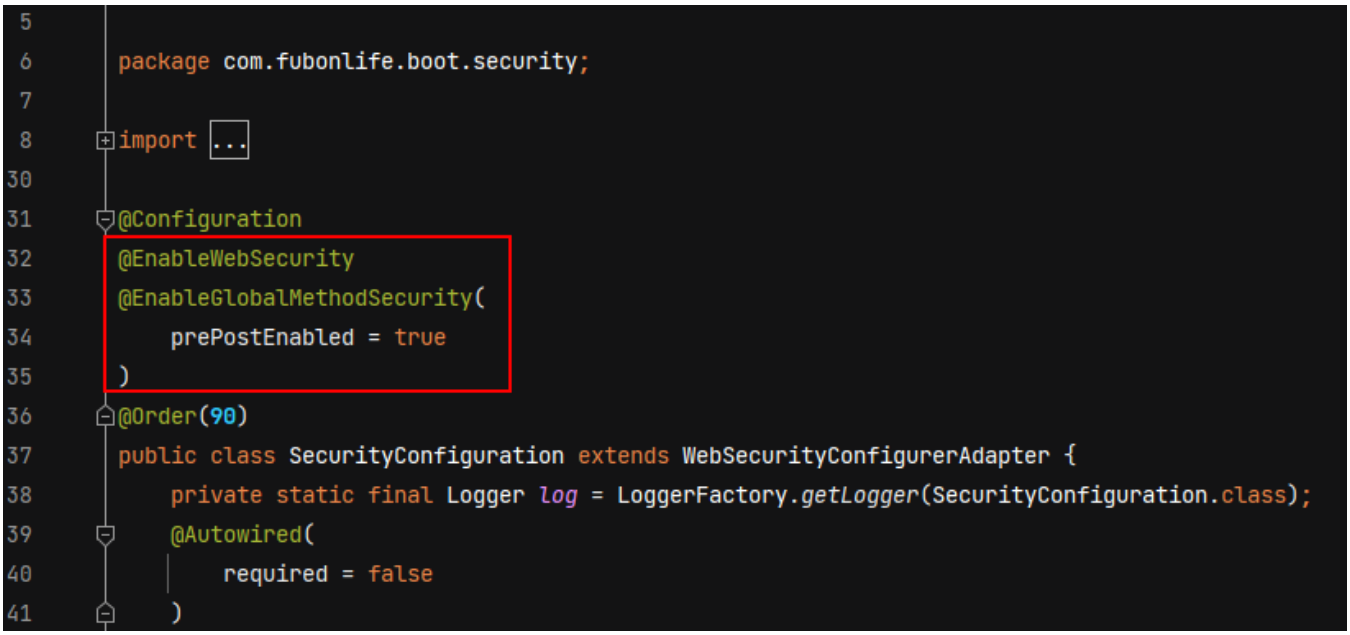
相關的程式

程式碼位置

- com.fubonlife.boot.jwt.JwtSecurityConfiguration.java
- com.fubonlife.boot.jwt.JwtAuthenticationTokenFilter.java

使用者授權 Authorize

啟用方式



```
5
6   package com.fubonlife.boot.security;
7
8   import ...
30
31  @Configuration
32  @EnableWebSecurity
33  @EnableGlobalMethodSecurity(
34      prePostEnabled = true
35  )
36  @Order(90)
37  public class SecurityConfiguration extends WebSecurityConfigurerAdapter {
38      private static final Logger log = LoggerFactory.getLogger(SecurityConfiguration.class);
39      @Autowired(
40          required = false
41      )
```

> *Method Annotation*
>
> - *@PreAuthorize 在方法調用前，用戶必須通過身分驗證*
> - *@PostAuthorize 方法調用後，如果表達式結果為 false，就會拋出安全性異常*

官方資料來源：27. Expression-Based Access Control (spring.io)

舉例說明

```
@GetMapping(value = "/me")
@ApiOperation("")
@PreAuthorize("isAuthenticated()") // , true
public AccountDto getMe() {
    Account account = authService.getCurrent();
    return modelMapper.map(account, AccountDto.class);
}


@ApiOperation("")
@PreAuthorize("isAnonymous()") // , true
public Account[] findAccounts();


@ApiOperation("")
@GetMapping("{id}")
@PreAuthorize("hasAnyRole('ROOT') or @customSecurity.iam(#id)") // , true
public AccountDto getAccount(@PathVariable String id) {
    return modelMapper.map(accountService.findById(id), AccountDto.class);
}


@PreAuthorize (" #book.owner == authentication.principal.username ")
public void deleteBook(Book book);

@PostAuthorize (" returnObject.owner == authentication.principal.username ")
public Book getBook();
```