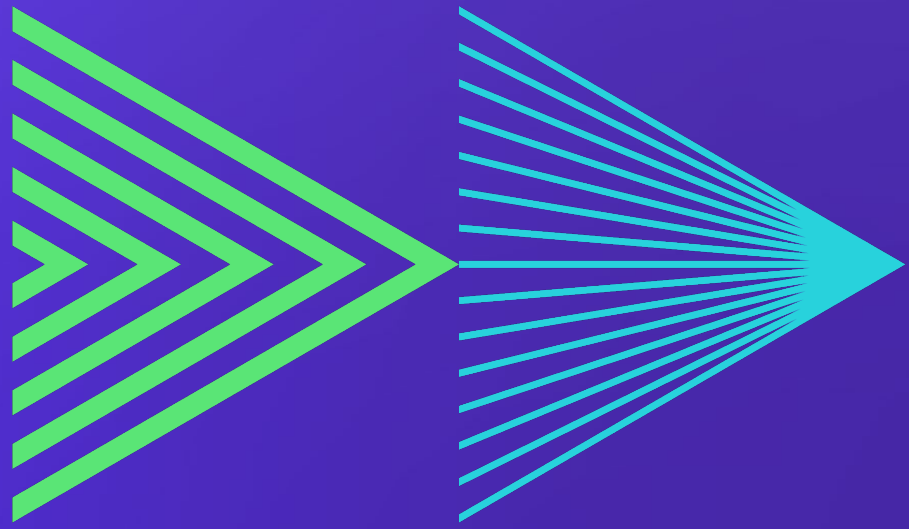
NHN FORWARD

오픈소스 KeyCloak을 활용한 인증 서버 구축기

NHN Dooray 결재서비스개발팀

서태진, 한덕선



다룰 내용

1. 왜 Keycloak일까?
2. Keycloak 사용한 기능
3. 발생한 이슈 및 해결
4. 개선 방향

왜 Keycloak일까?

Single-Sign On

한 번의 로그인으로 여러 가지 사이트를 이용

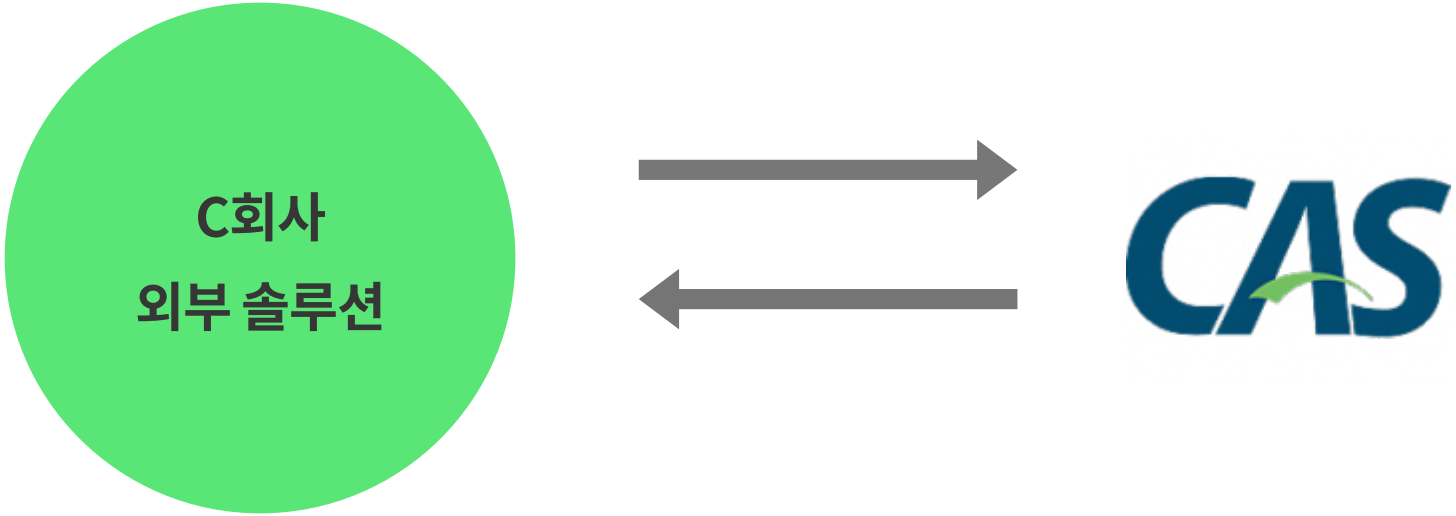
기존 인증

기존 인증

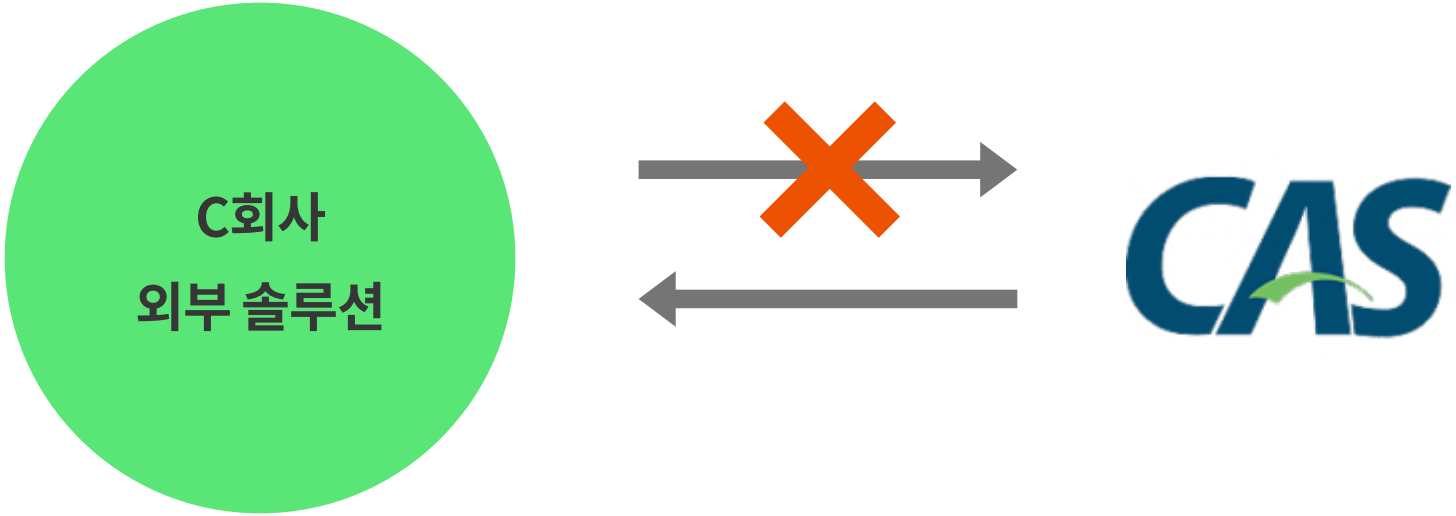
C회사
외부 솔루션

CAS

기존 인증



기존 인증



OpenSource SSO 비교

JAVA

JAVA

C#

OpenSource SSO 비교

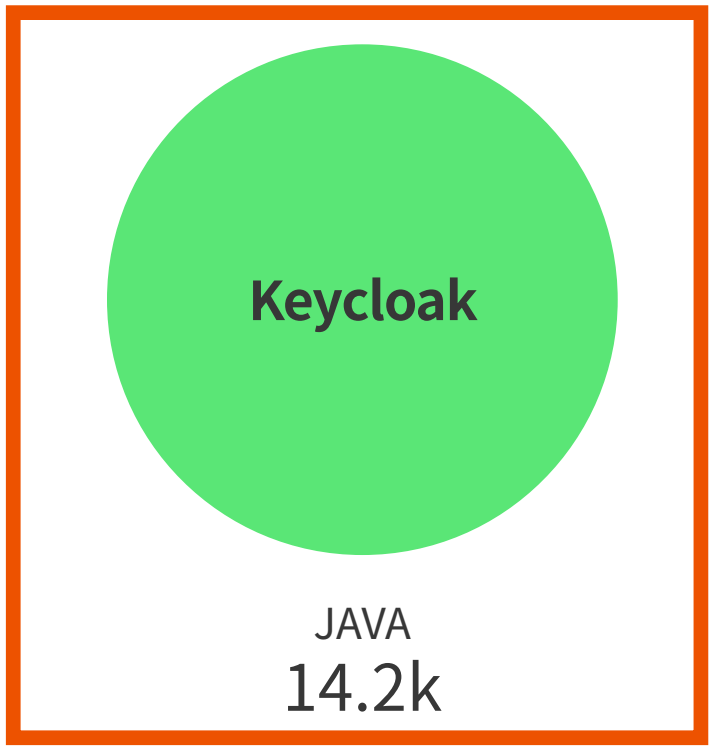
JAVA
14.2k

JAVA
9.8k

C#
8.9k

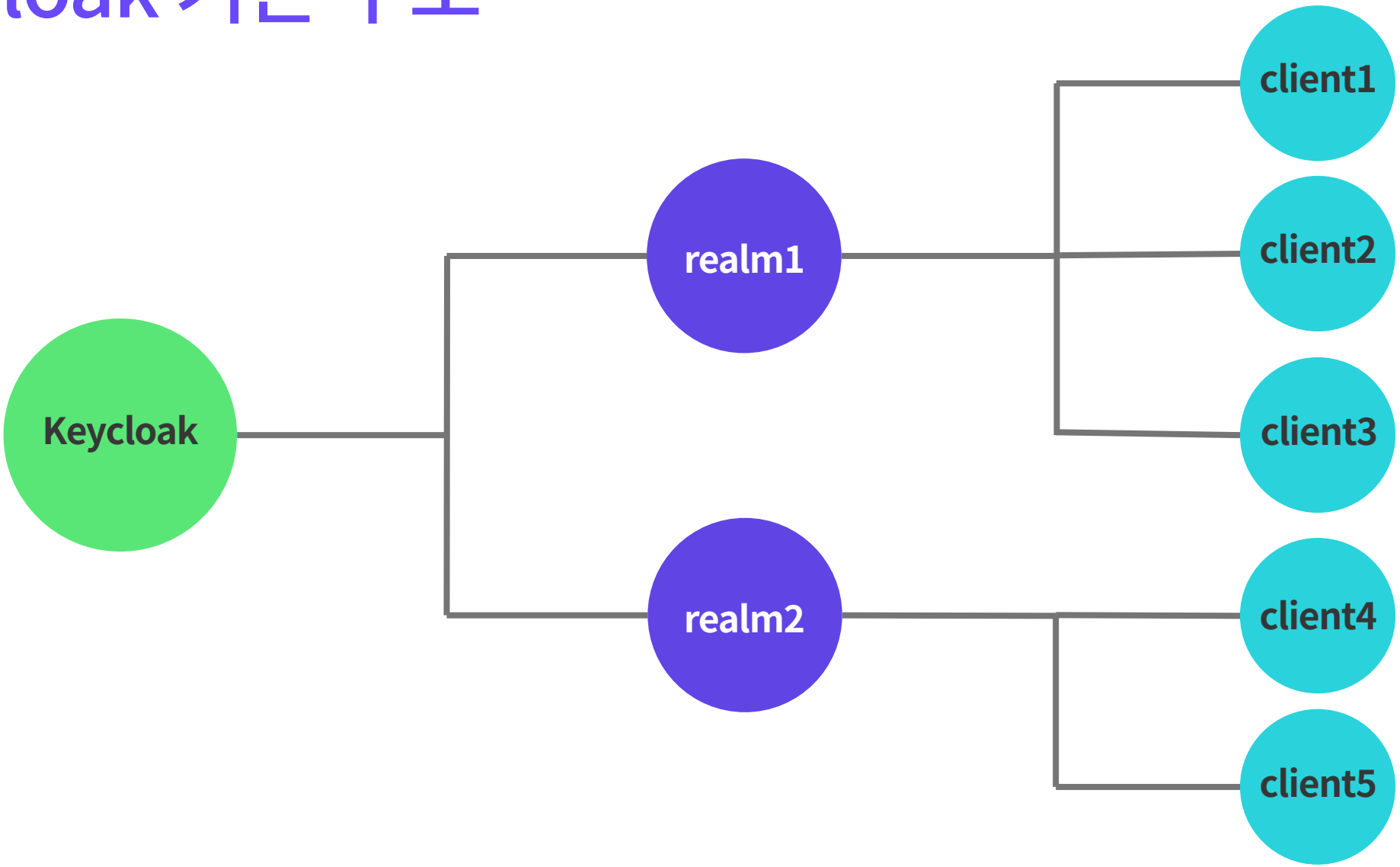
OpenSource SSO 비교

결정



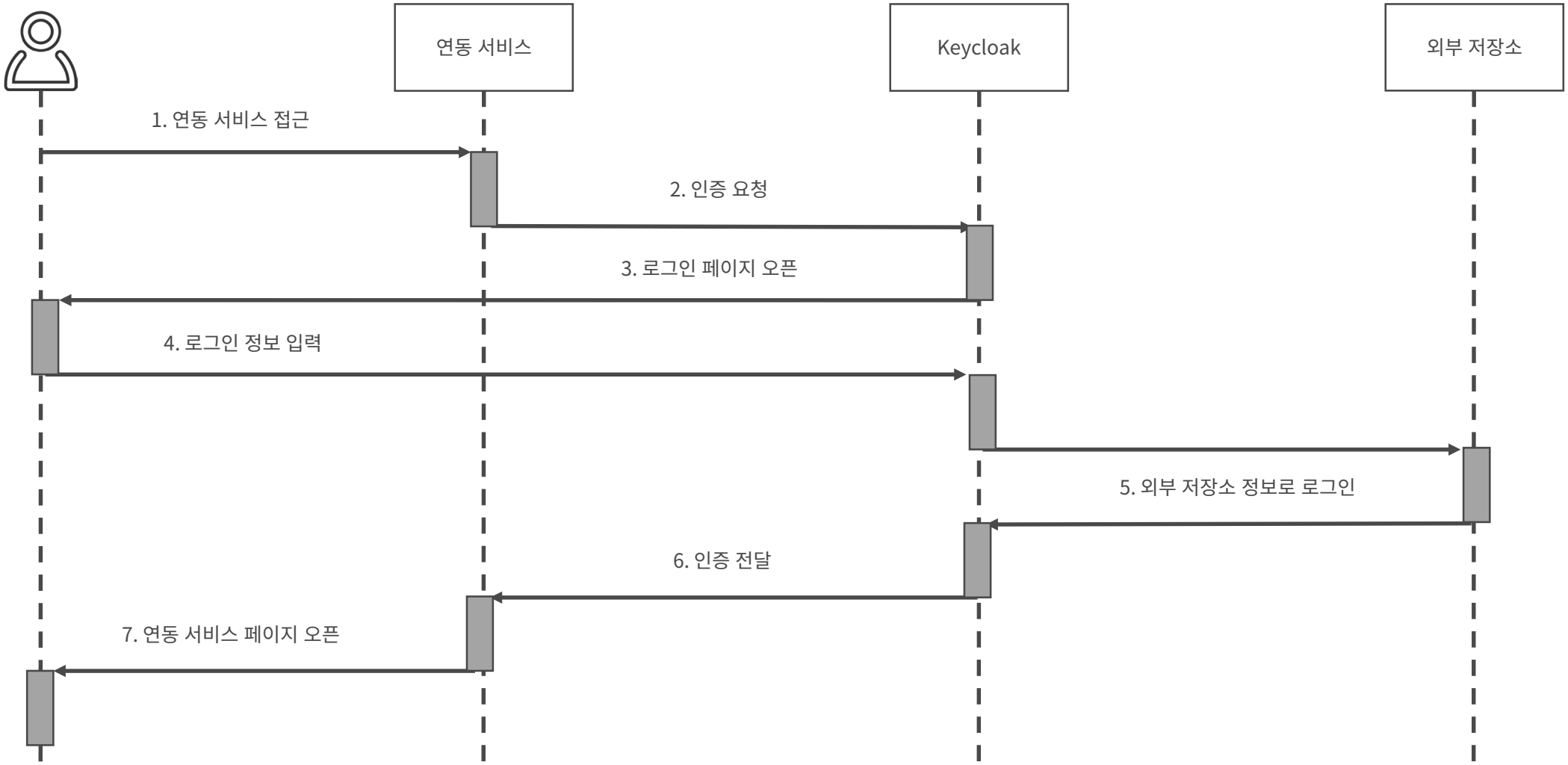
Keycloak 사용한 기능

Keycloak 기본 구조



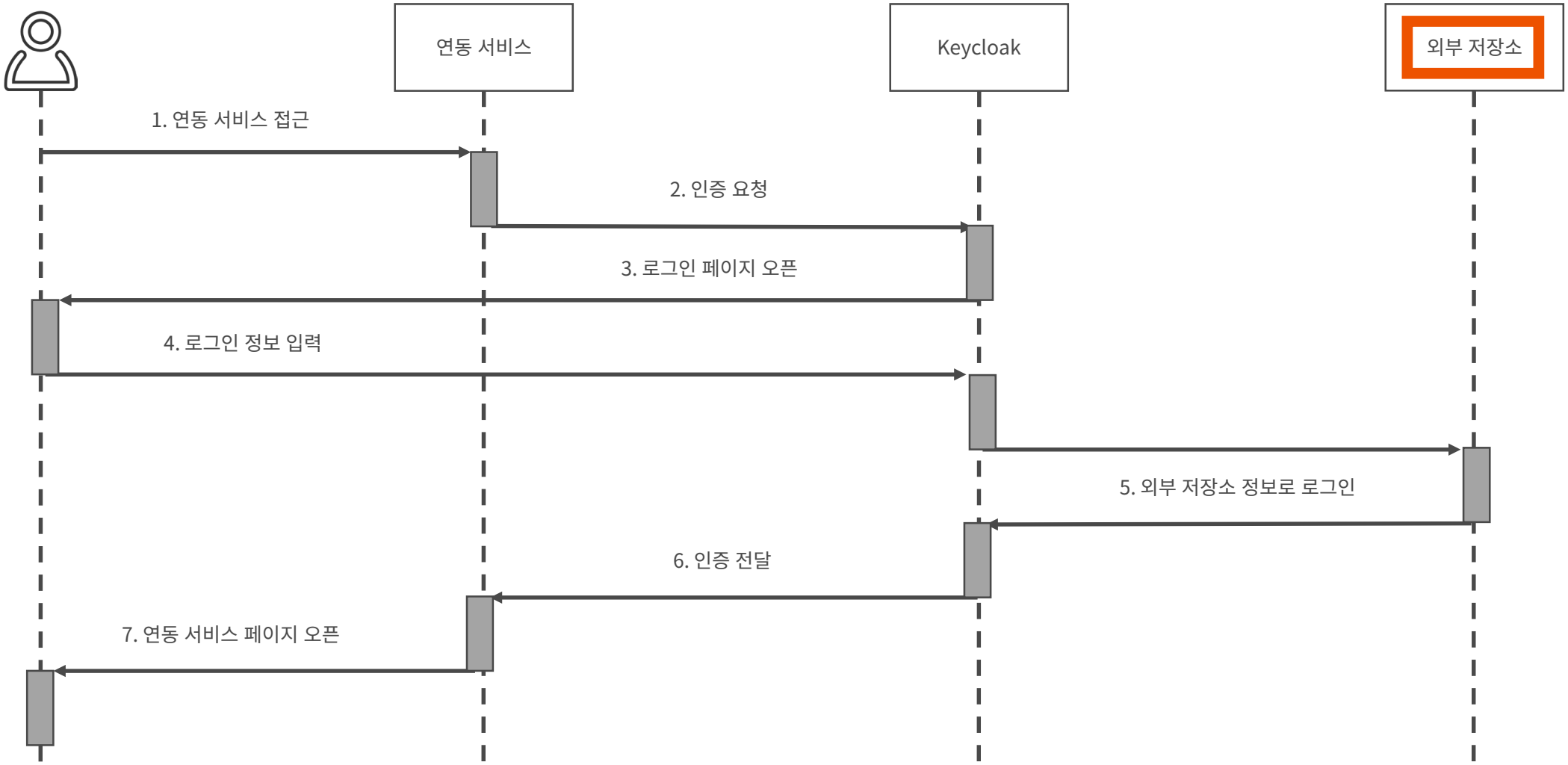
Keycloak 로그인 과정

NHN FORWARD



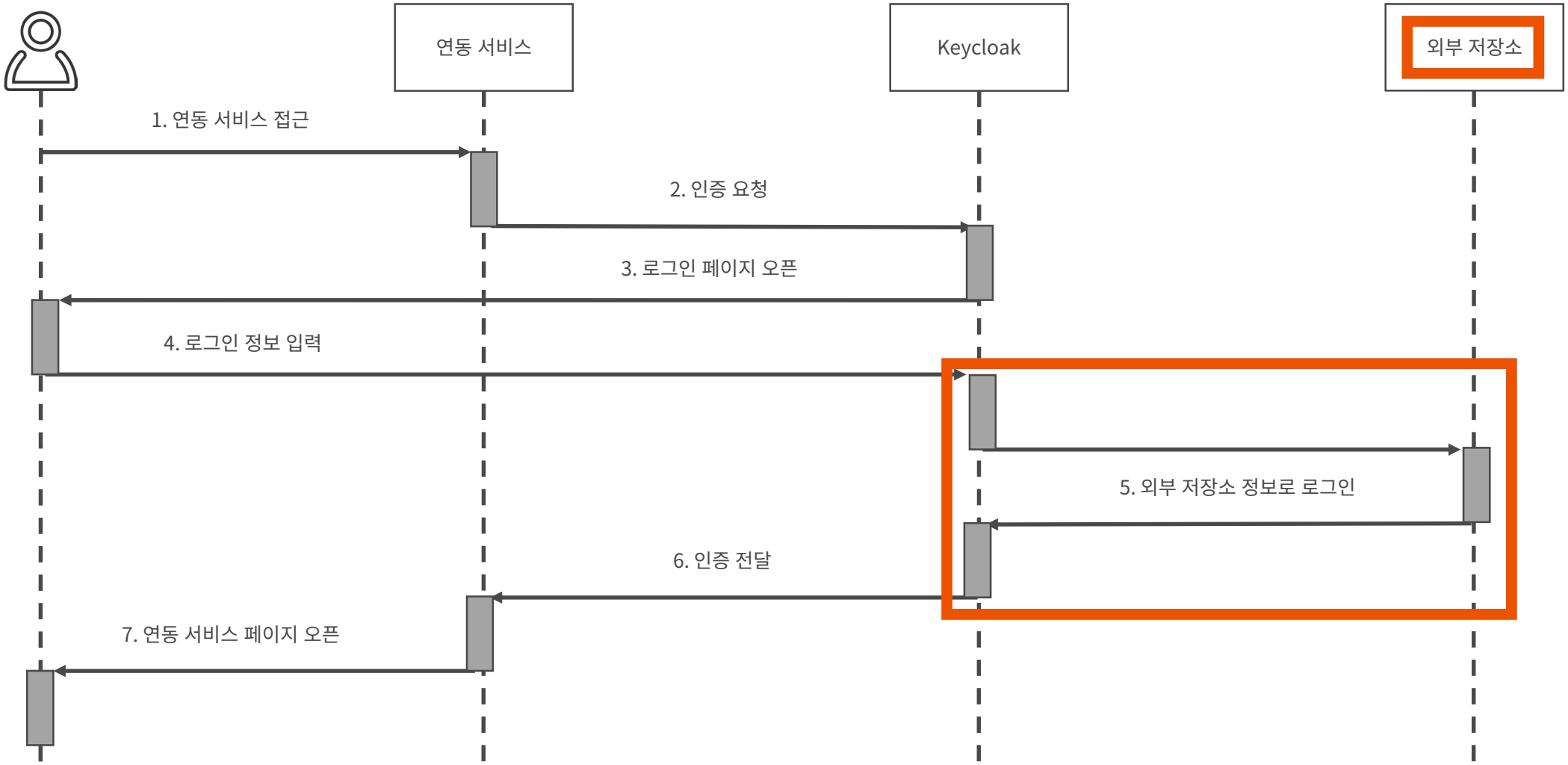
Keycloak 로그인 과정

NHN FORWARD



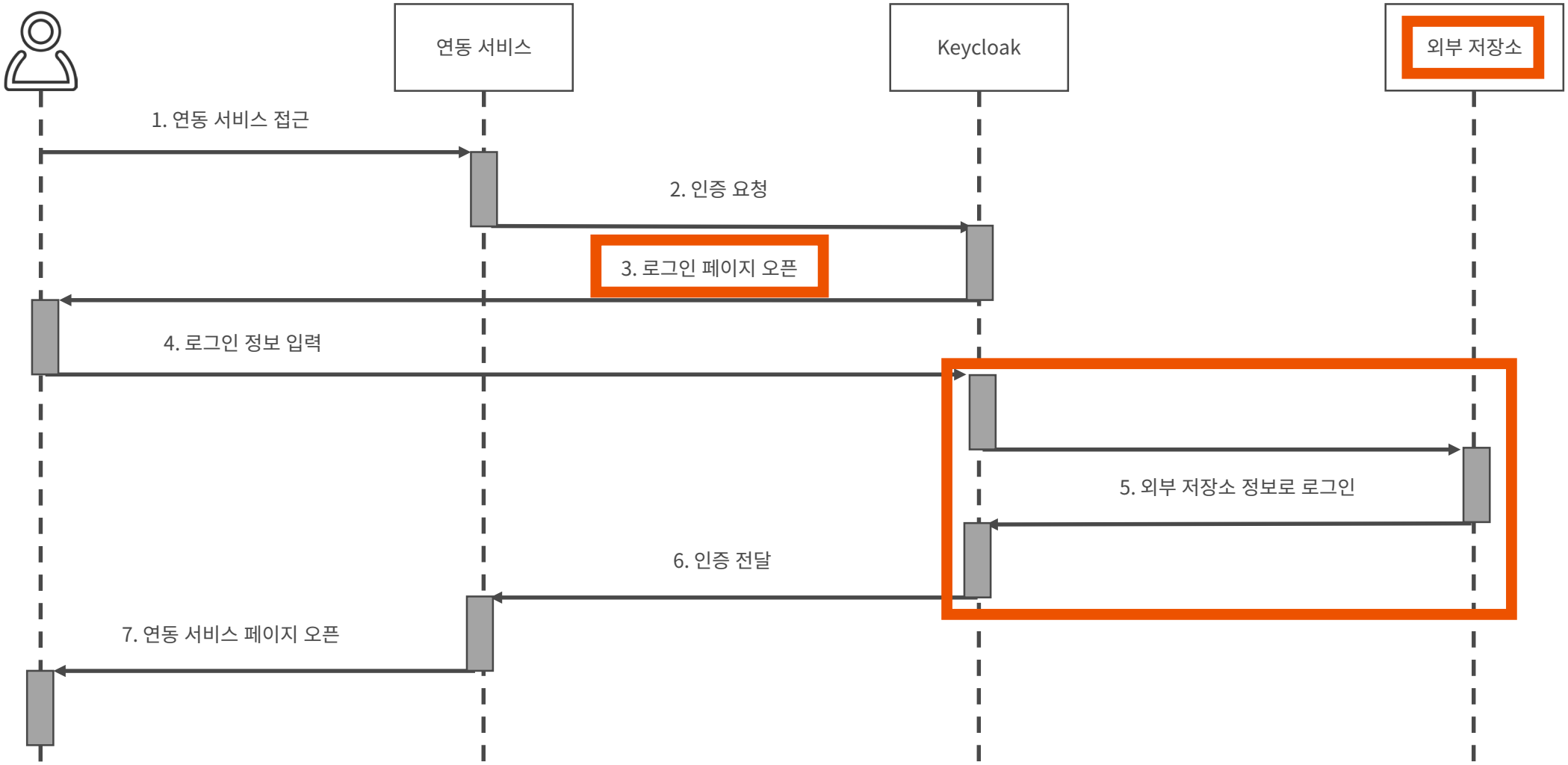
Keycloak 로그인 과정

NHN FORWARD



Keycloak 로그인 과정

NHN FORWARD

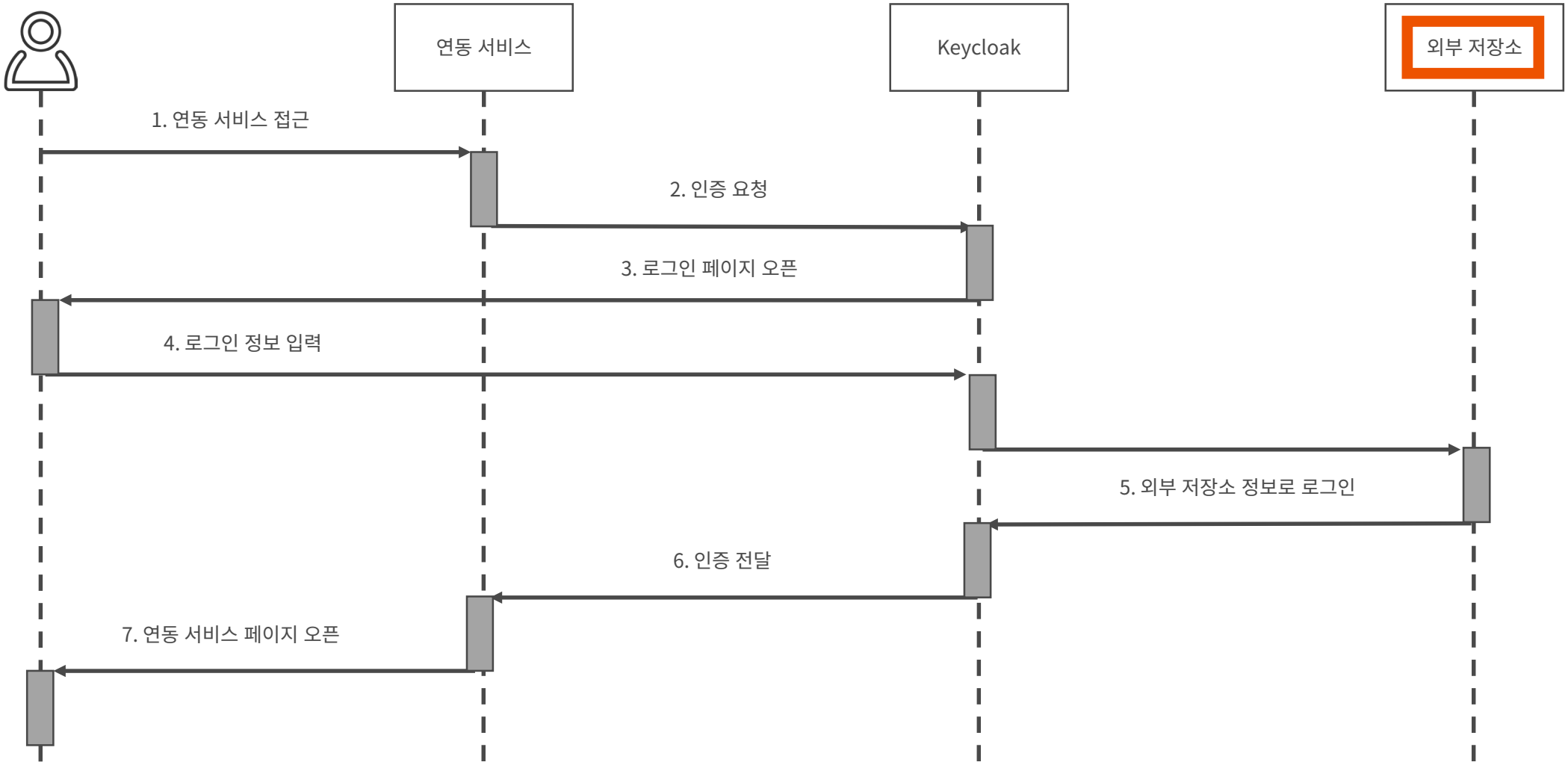


User Storage Federation

NHN FORWARD

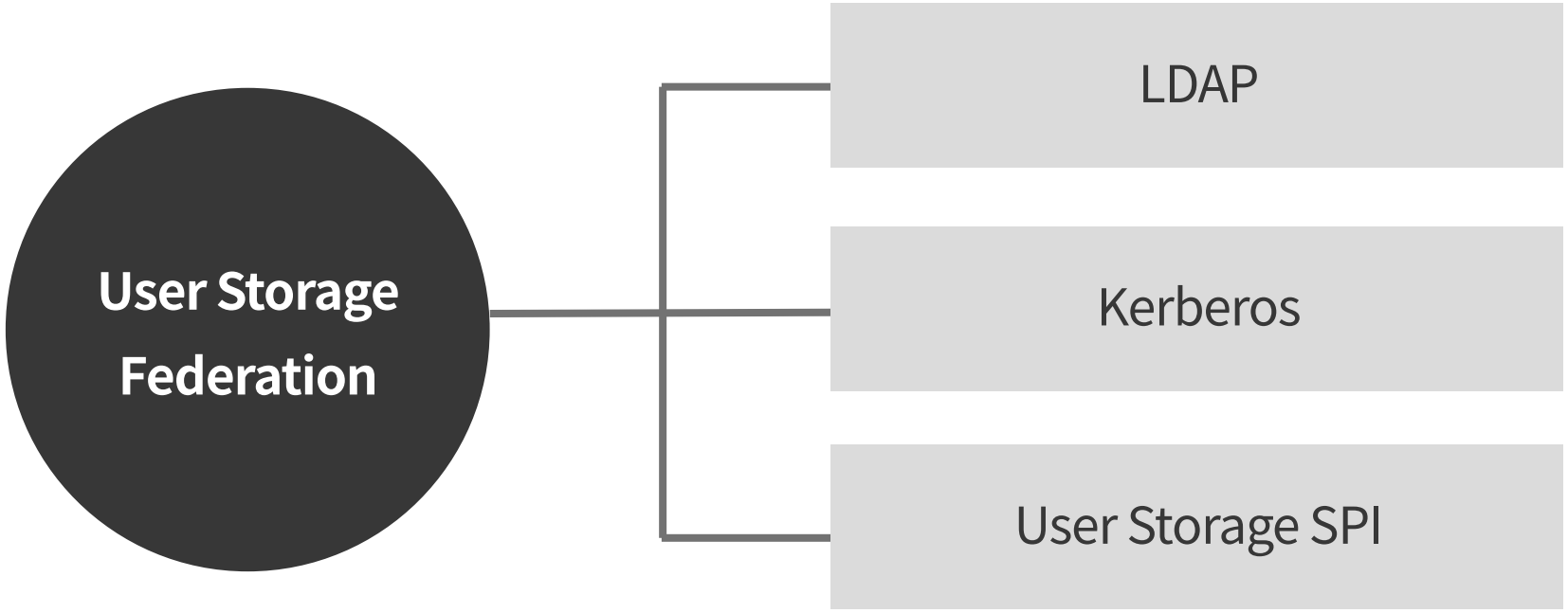
User Storage Federation

NHN FORWARD



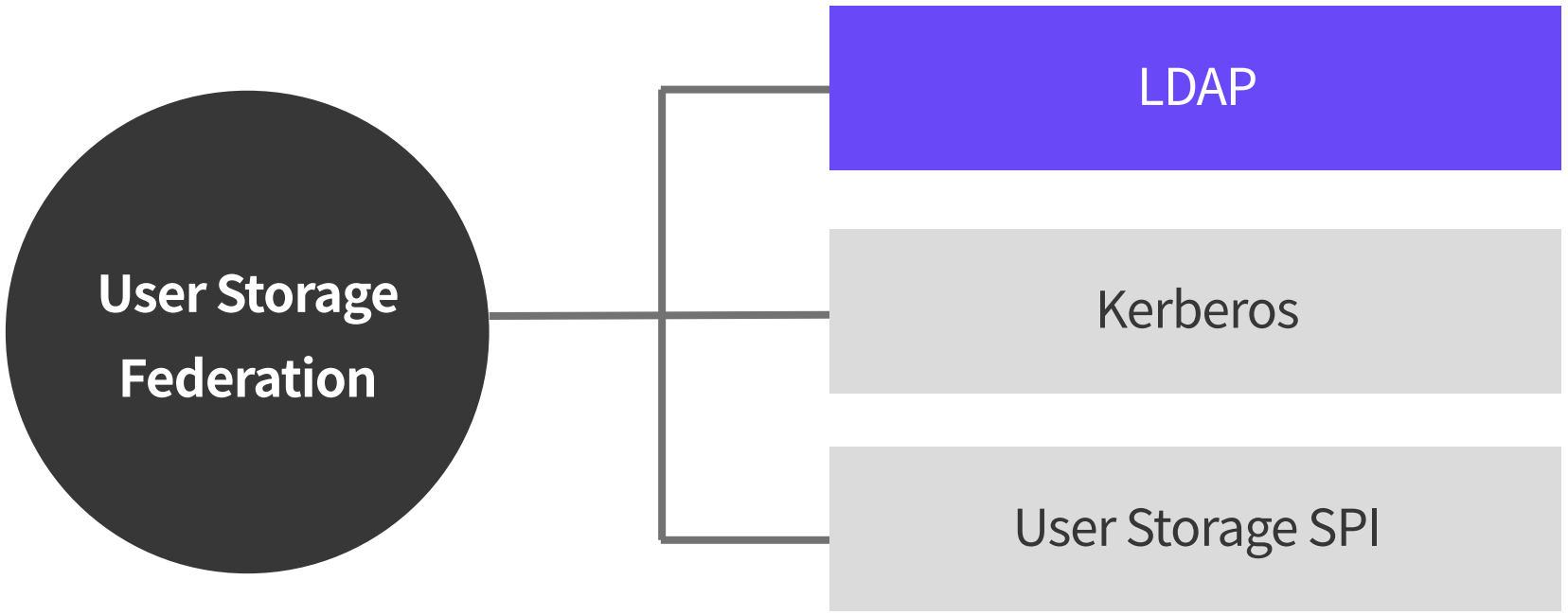
User Storage Federation

3가지 연동 방식



User Storage Federation

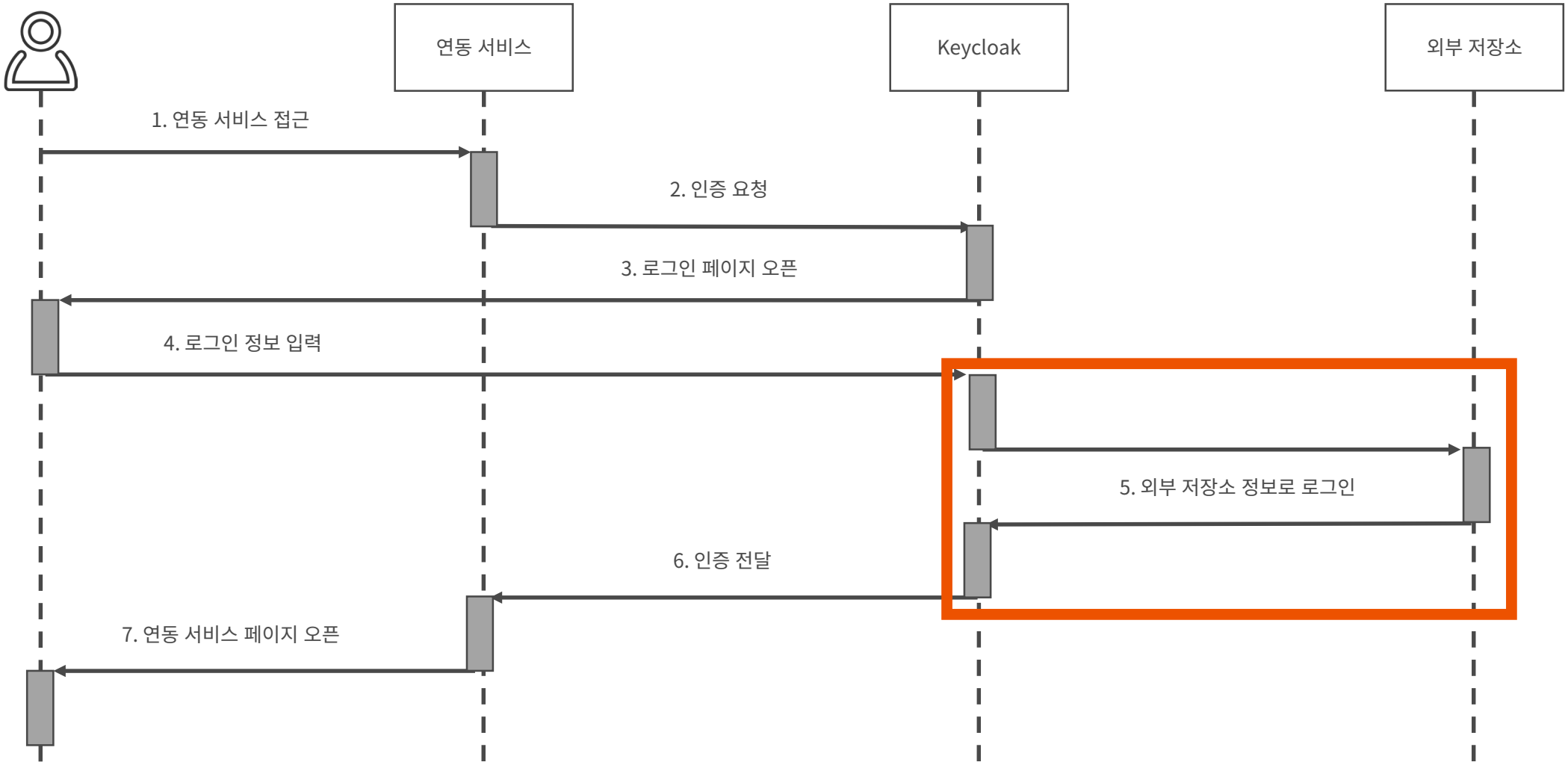
3가지 연동 방식



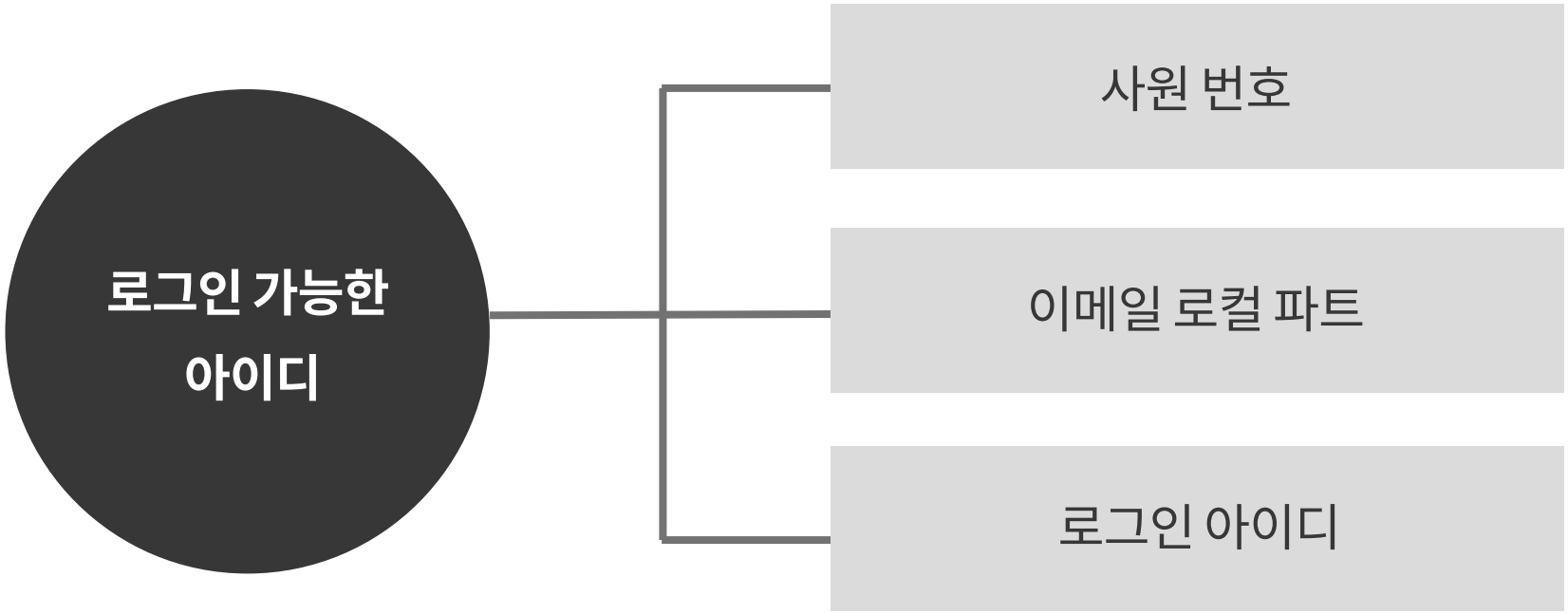
Authentication SPI

Authentication SPI

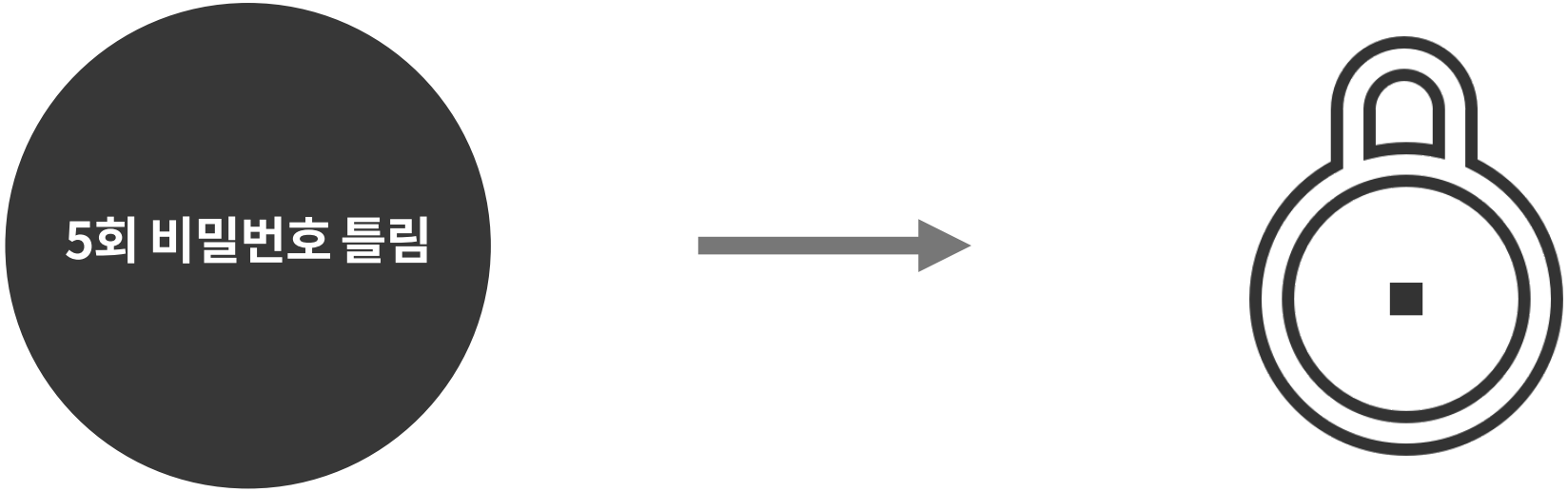
NHN FORWARD



Authentication SPI



Authentication SPI



Authentication SPI

NHN FORWARD

임시 잠금 계정
로그인 시도

Authentication SPI

NHN FORWARD

잠금 계정
로그인 시도

▸계정잠김

사내시스템 사용이 다음과 같은 사유로 접근이 차단되었습니다.

1. 임시 계정이 만료된 경우

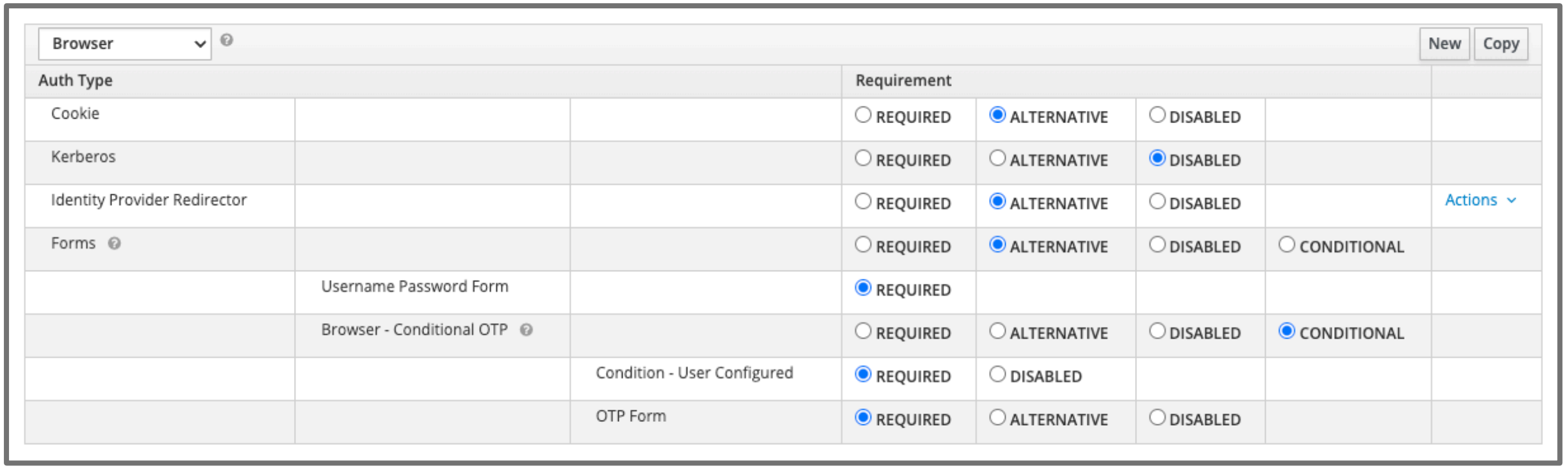
2. 기타 보안상의 사유로 연결이 일시적으로 차단된 경우

〔관련 문의 : 사내정보시스템_운영([redacted]@nhn.com)〕

Authentication SPI

NHN FORWARD

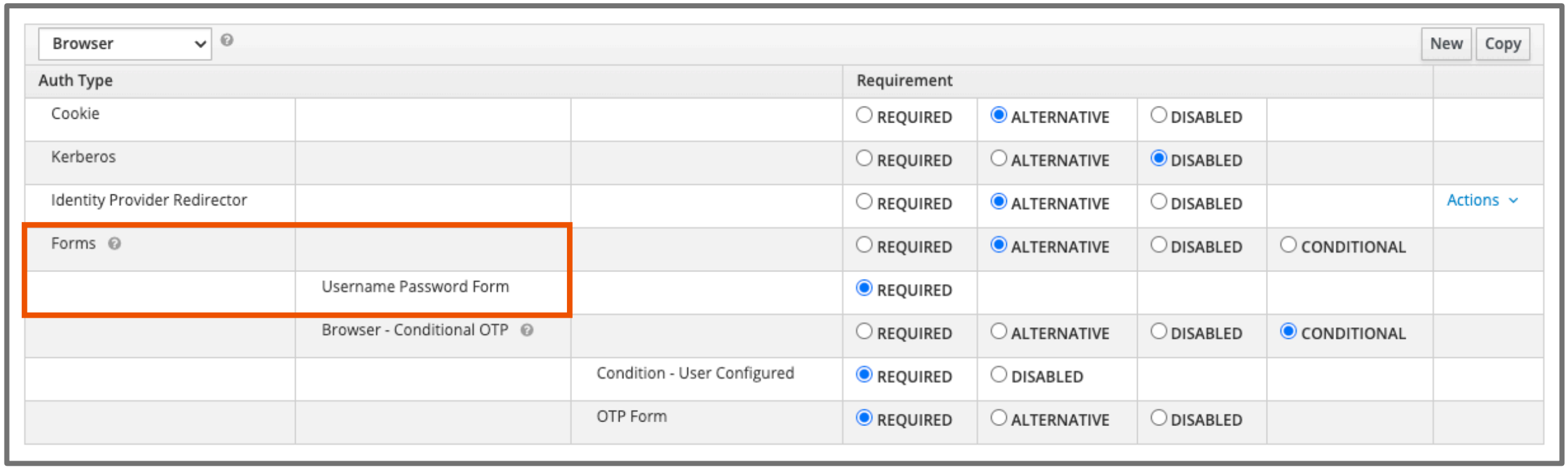
Authentication > Flows > Browser



Authentication SPI

NHN FORWARD

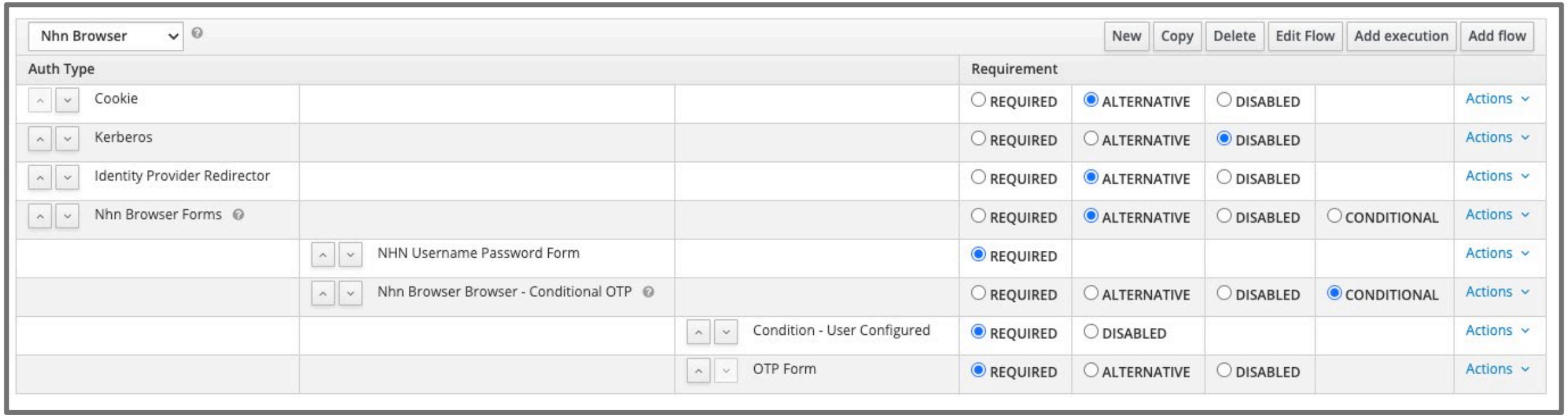
Authentication > Flows > Browser



Authentication SPI

NHN FORWARD

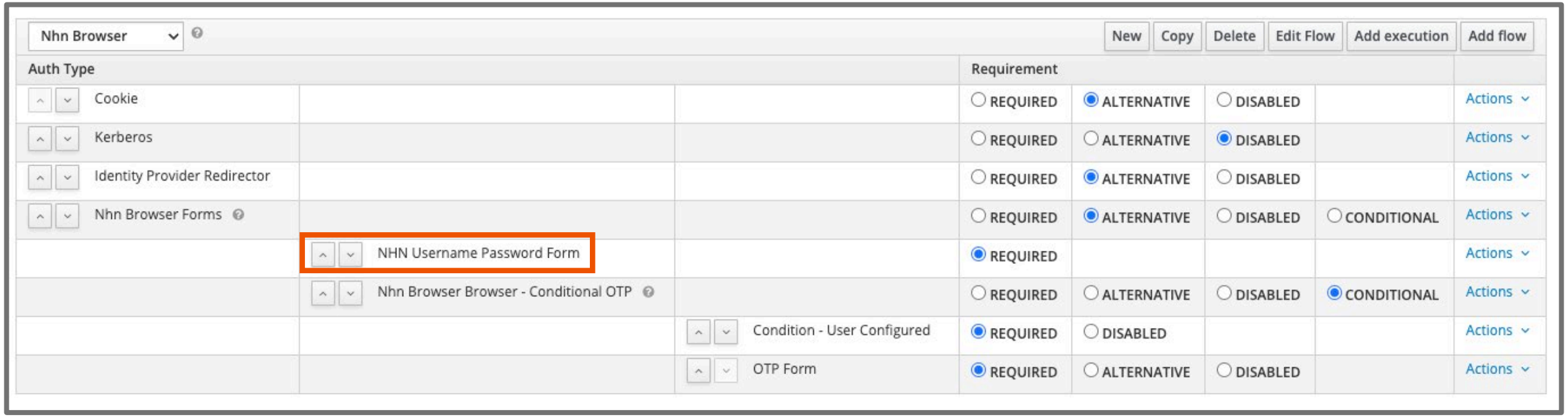
Authentication SPI 적용



Authentication SPI

NHN FORWARD

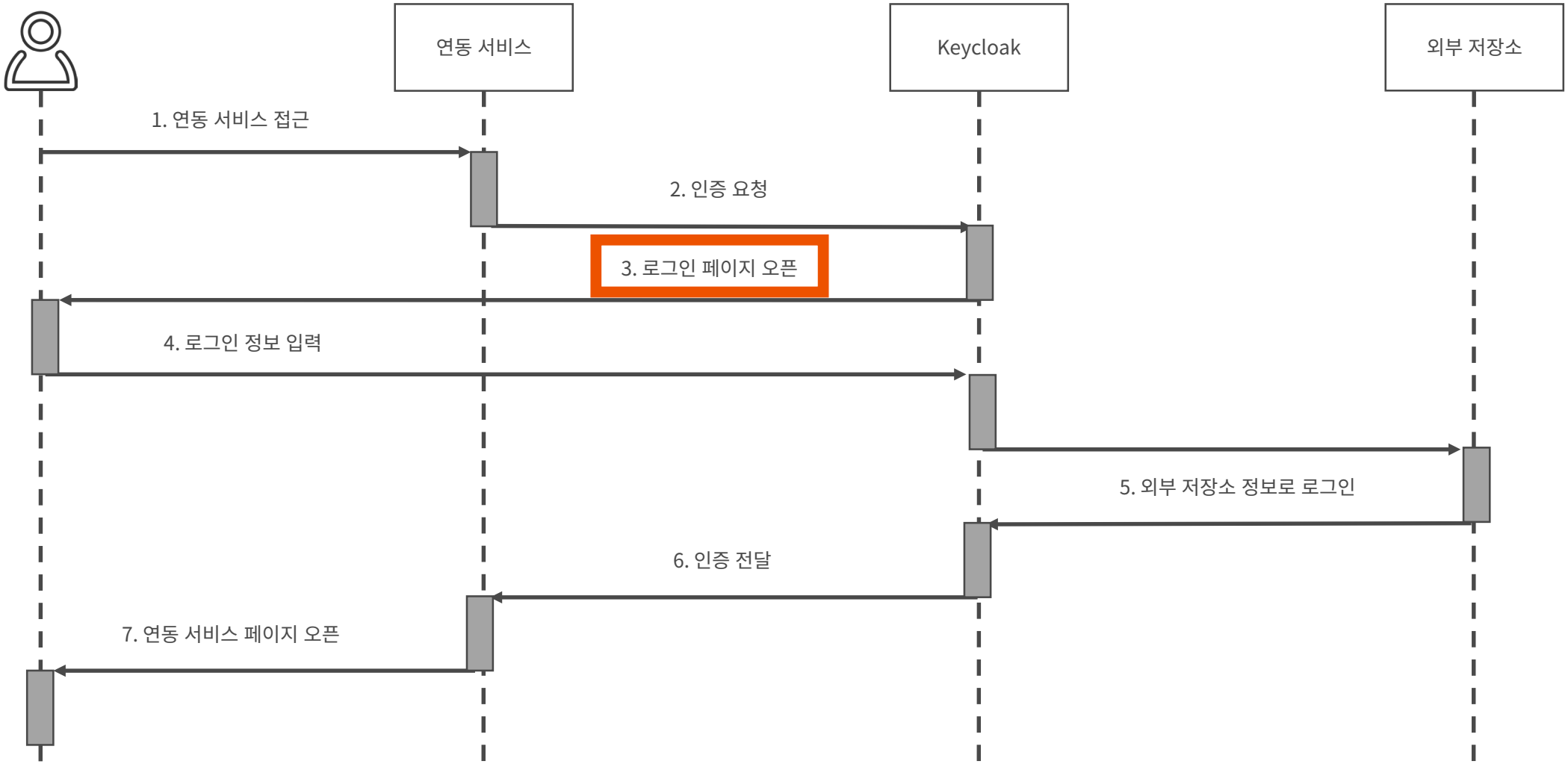
Authentication SPI 적용



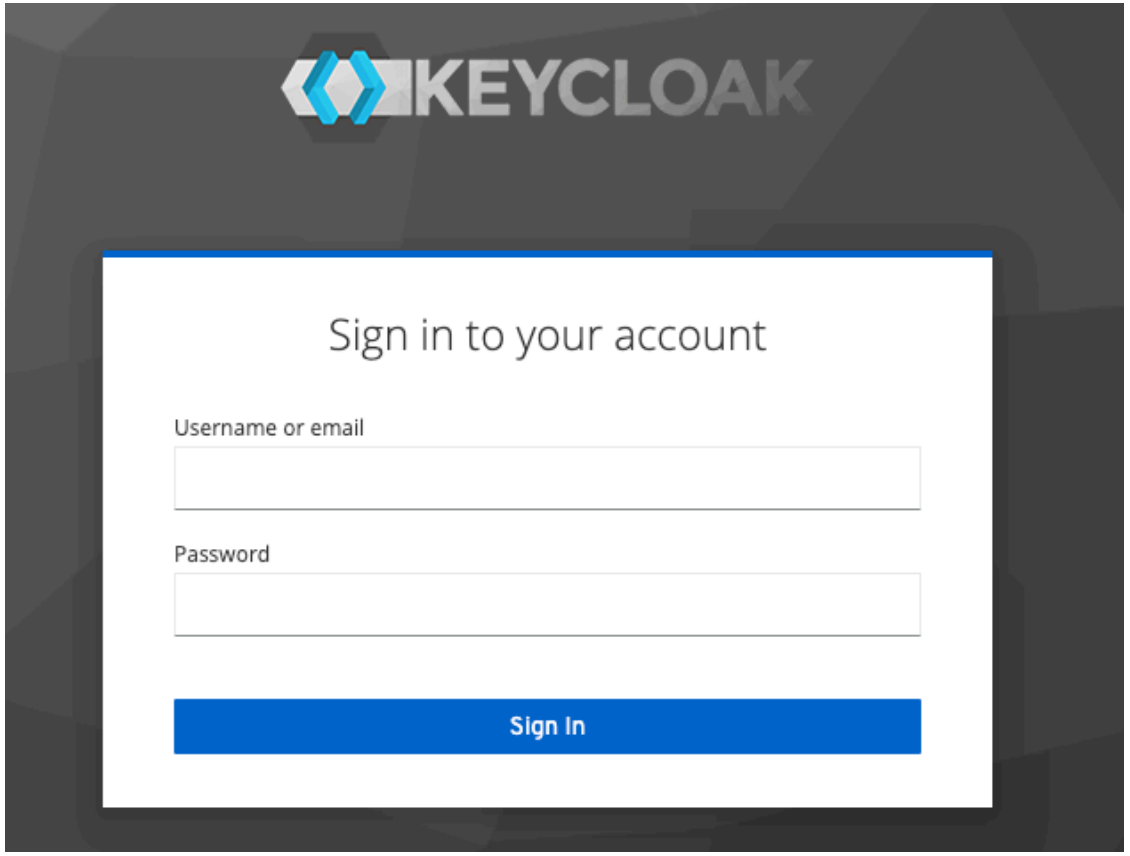
로그인 페이지

로그인 페이지

NHN FORWARD



로그인 페이지

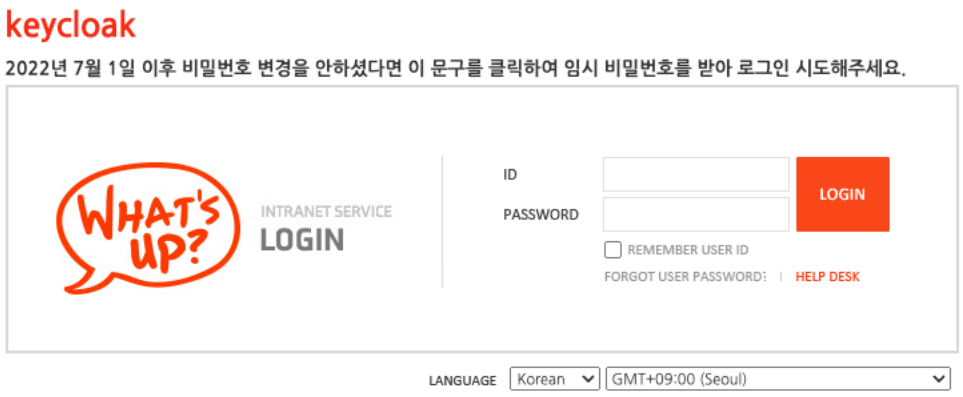

KEYCLOAK
Sign in to your account
Username or email
Password
Sign In

로그인 페이지

NHN FORWARD

로그인 페이지

NHN FORWARD

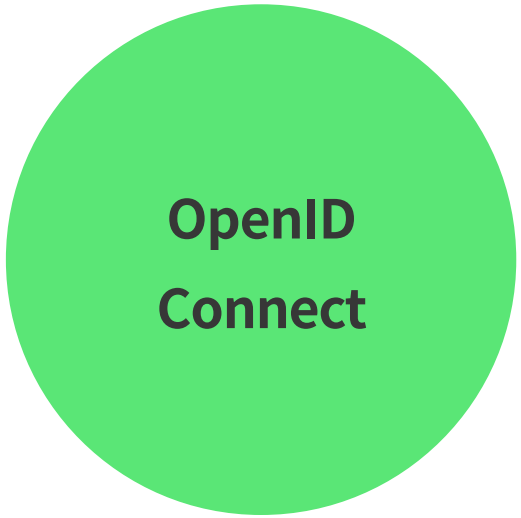


연동 방식

OpenID Connect

SAML

연동 방식

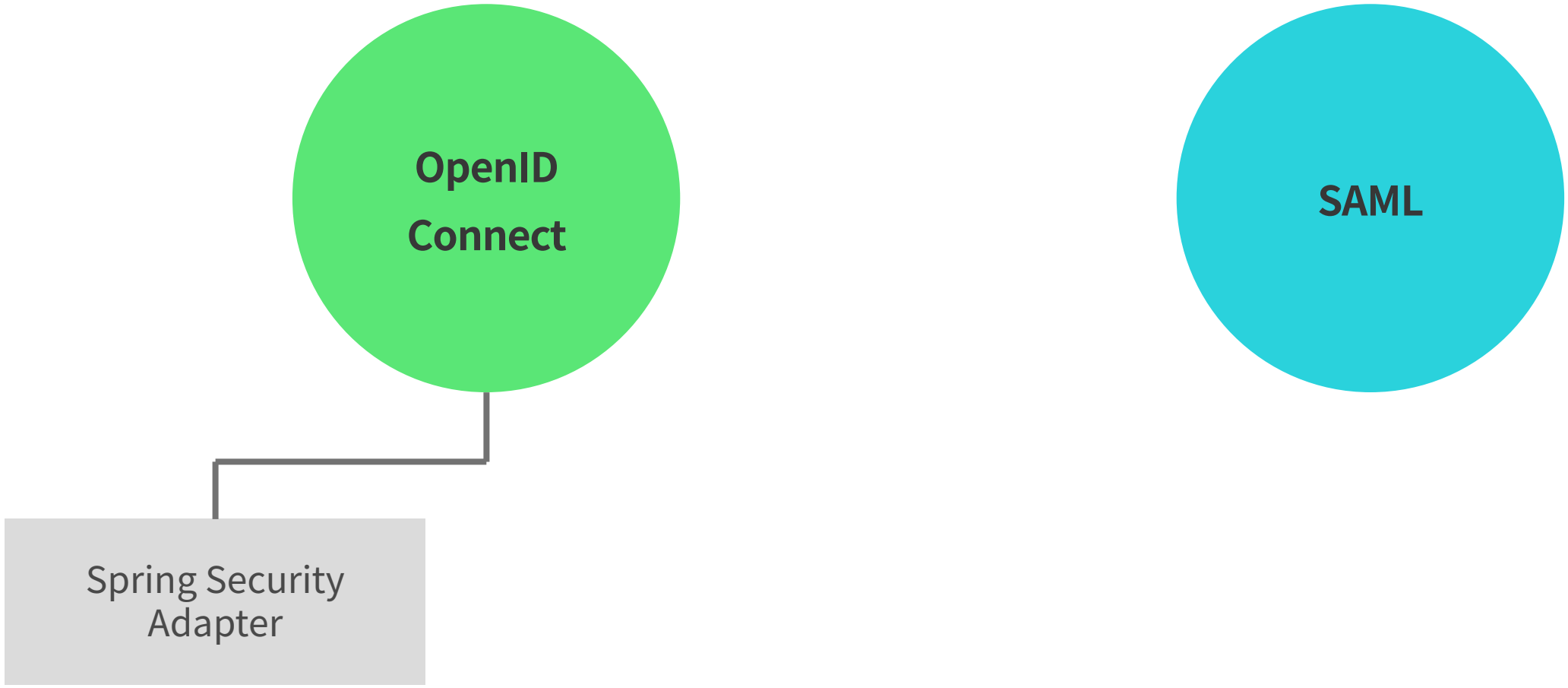


연동 방식

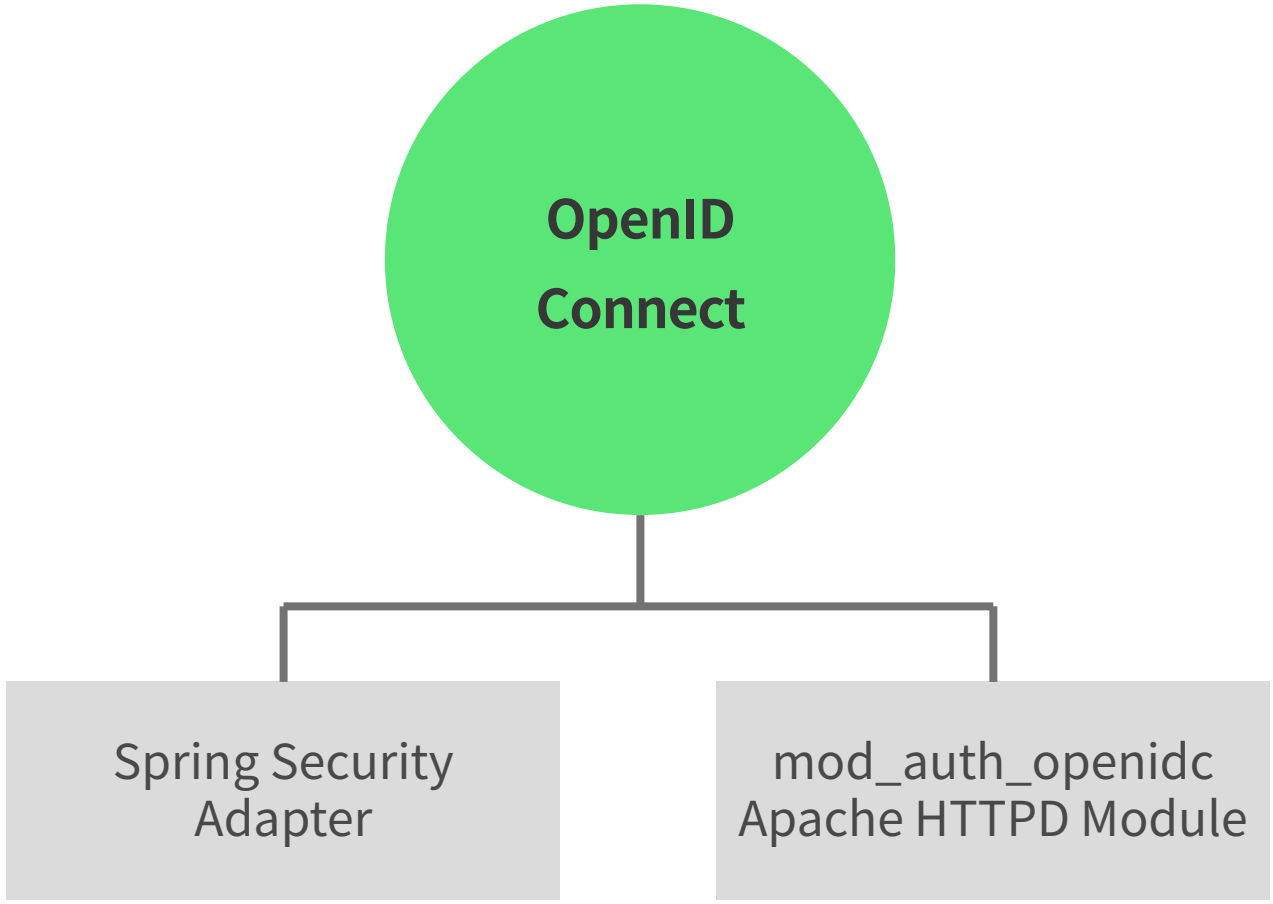
OpenID Connect

SAML

연동 방식

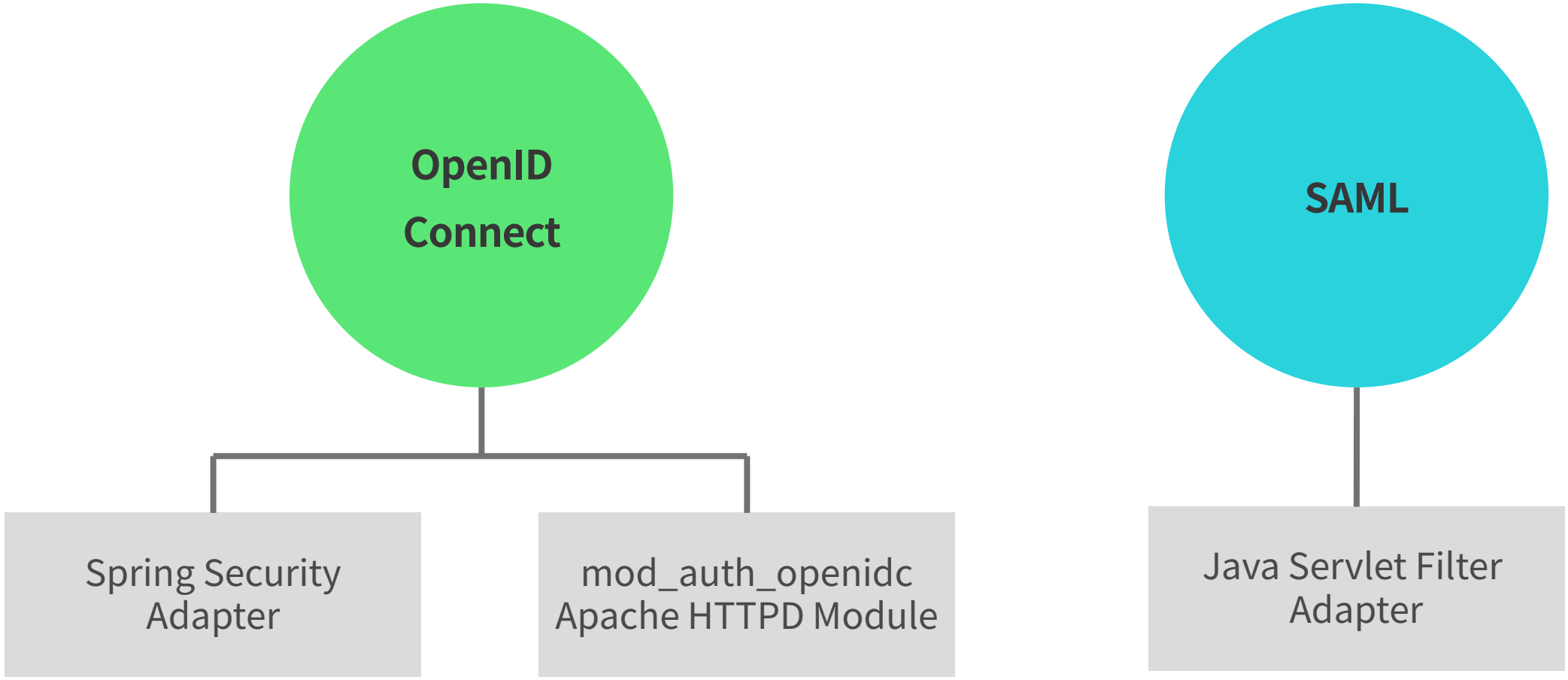


연동 방식


OpenID
Connect
Spring Security
Adapter
mod_auth_openidc
Apache HTTPD Module


SAML

연동 방식

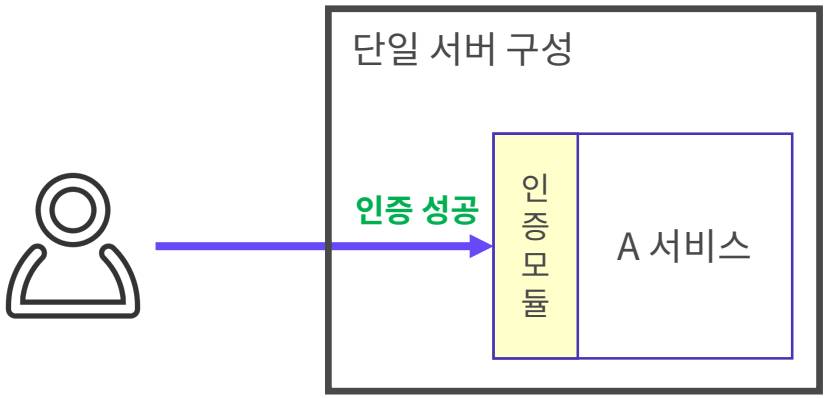

OpenID Connect
SAML
Spring Security Adapter
mod_auth_openidc Apache HTTPD Module
Java Servlet Filter Adapter

발생한 이슈 및 해결

이슈1: 서버 환경 구성

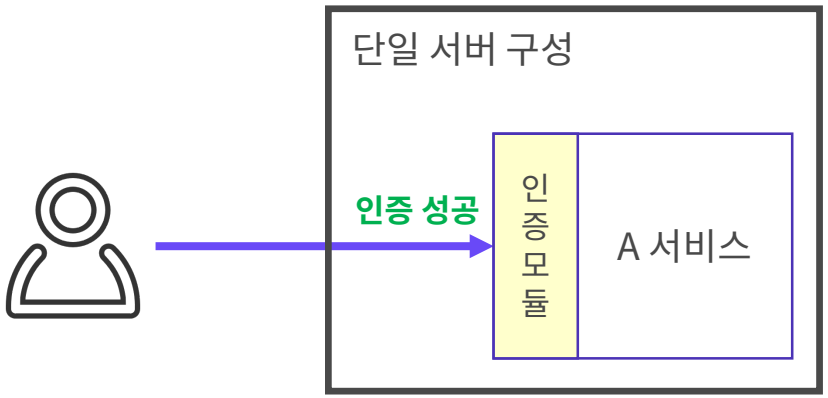
이슈1: 서버 환경 구성

DEV

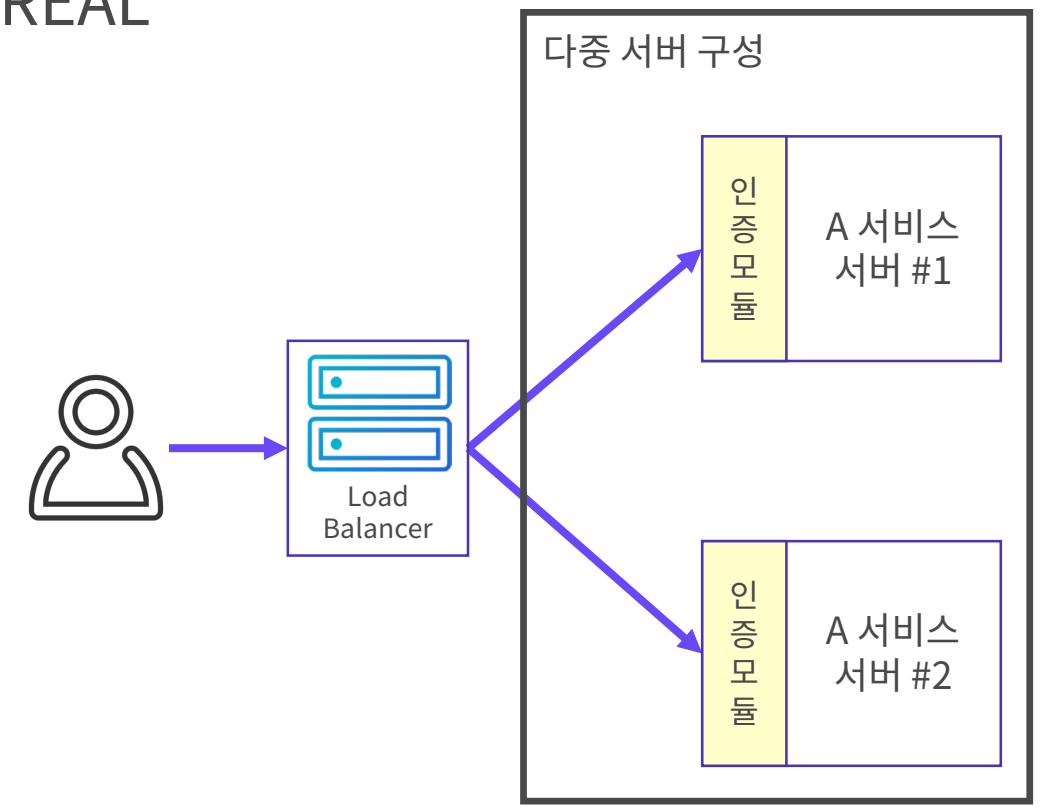


이슈1: 서버 환경 구성

DEV

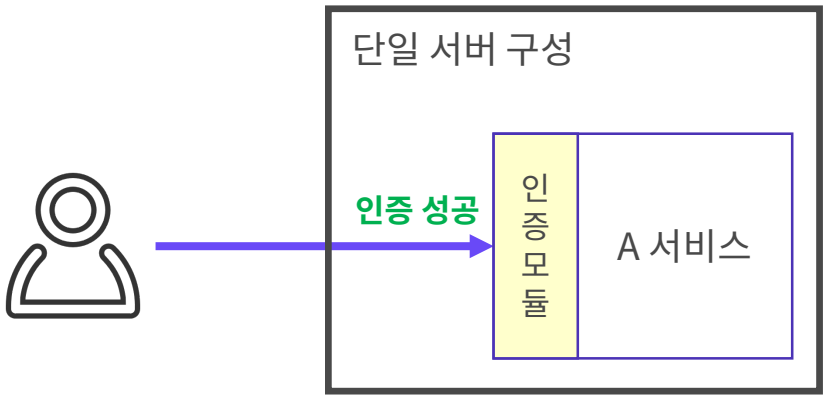


REAL

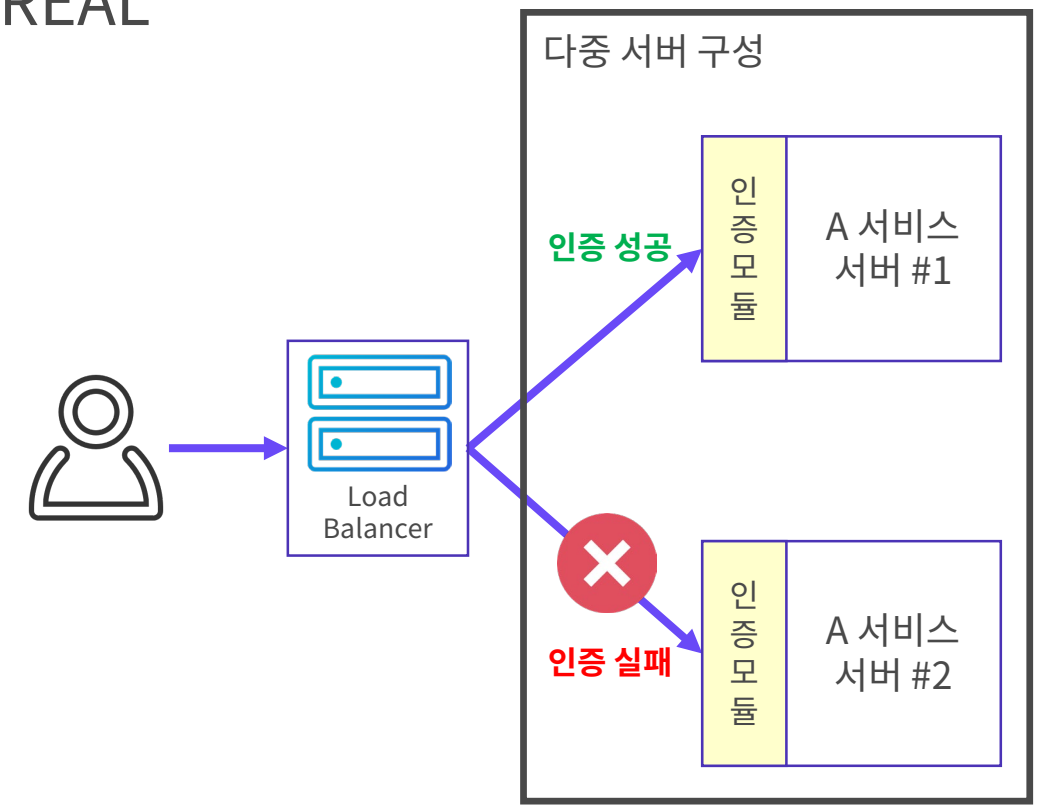


이슈1: 서버 환경 구성

DEV

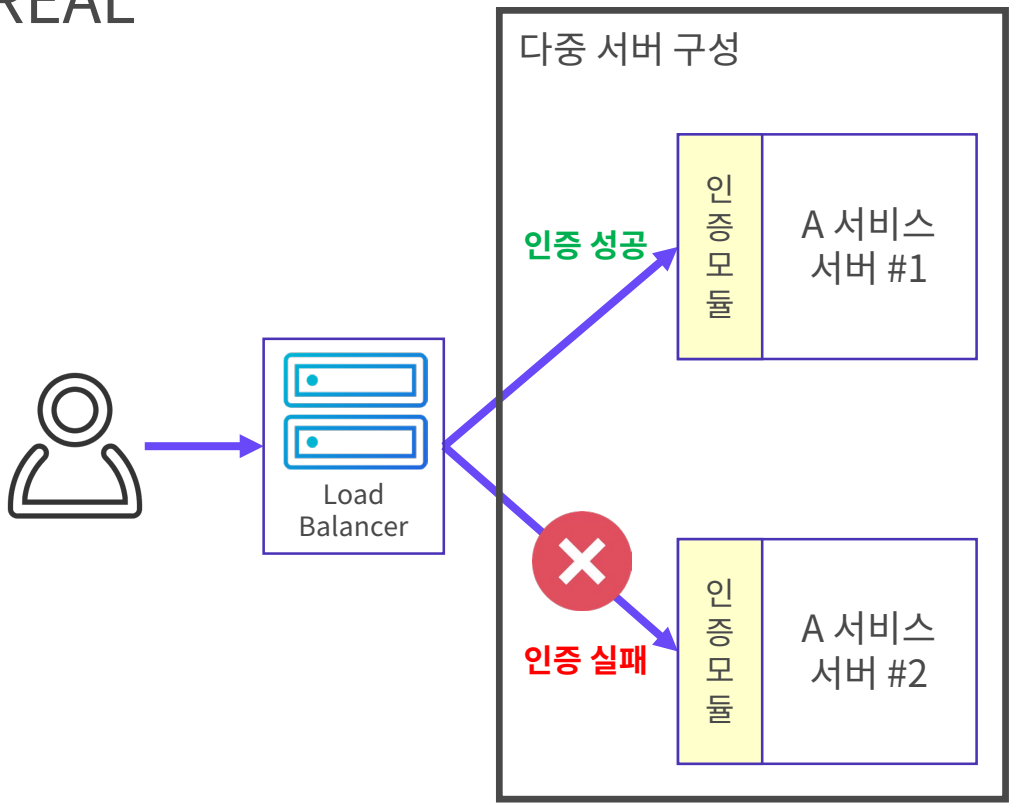


REAL



이슈1: 서버 환경 구성

REAL



이슈1: 서버 환경 구성

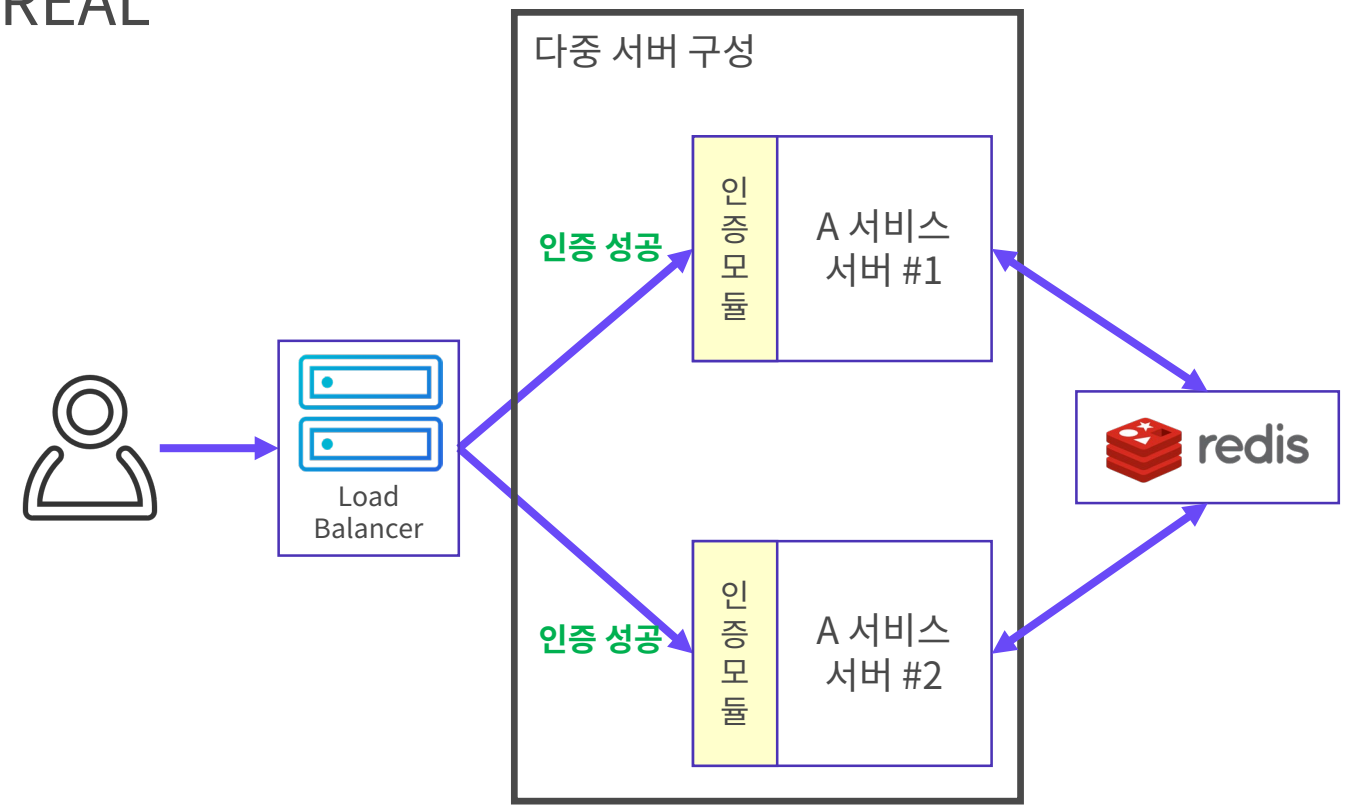
해결완료

이슈1: 서버 환경 구성

해 결 완 료

NHN FORWARD

REAL

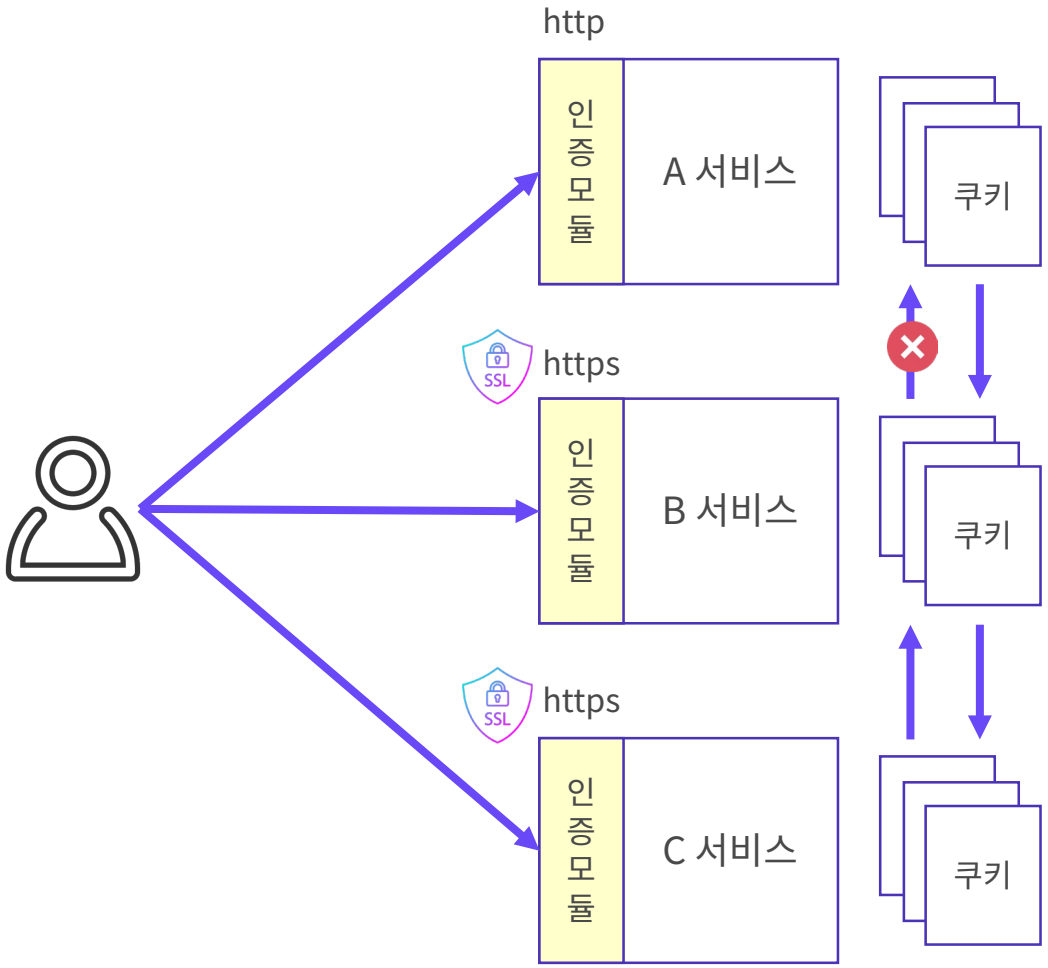


redis 적용

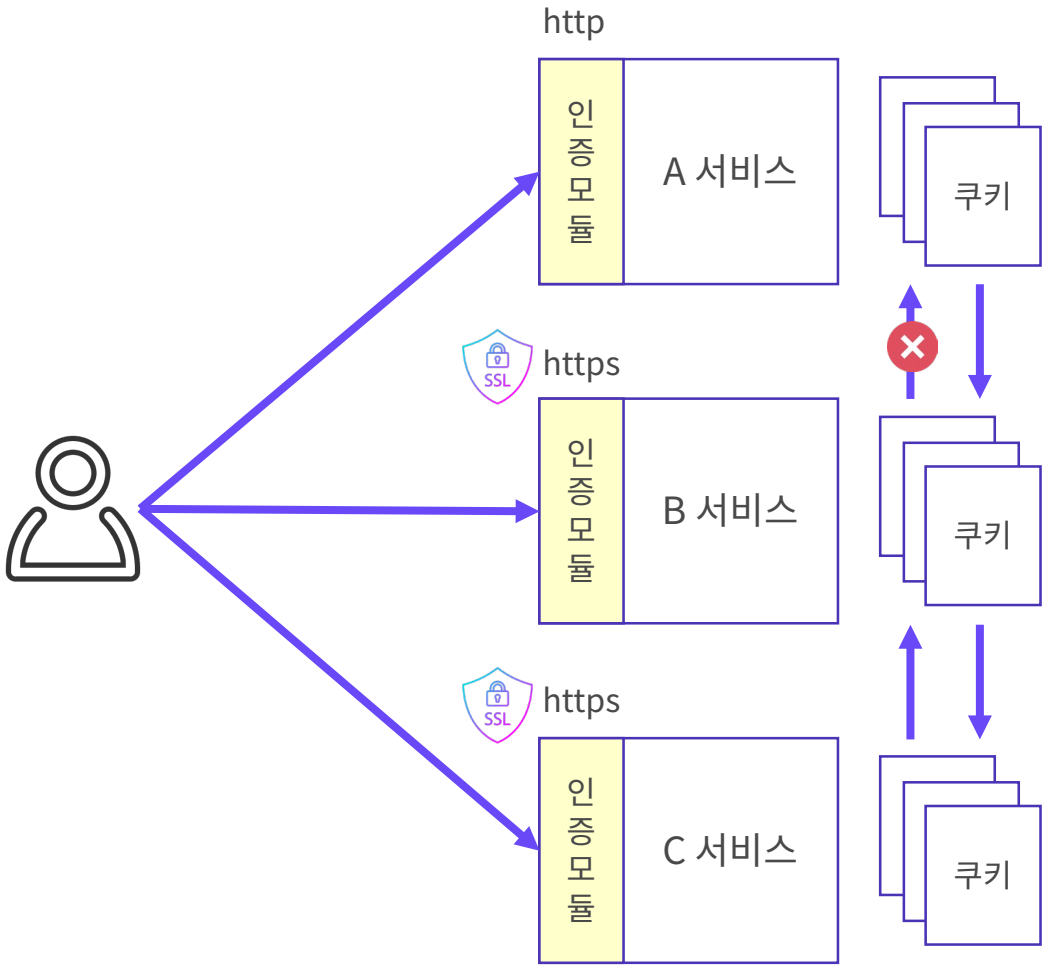
세션 공유를 통한 인증 정보 공유

이슈2: 쿠키 공유

이슈2: 쿠키 공유


http
인증모듈
A 서비스
쿠키
SSL
https
인증모듈
B 서비스
쿠키
SSL
https
인증모듈
C 서비스
쿠키

이슈2: 쿠키 공유



http → https 인지 실패

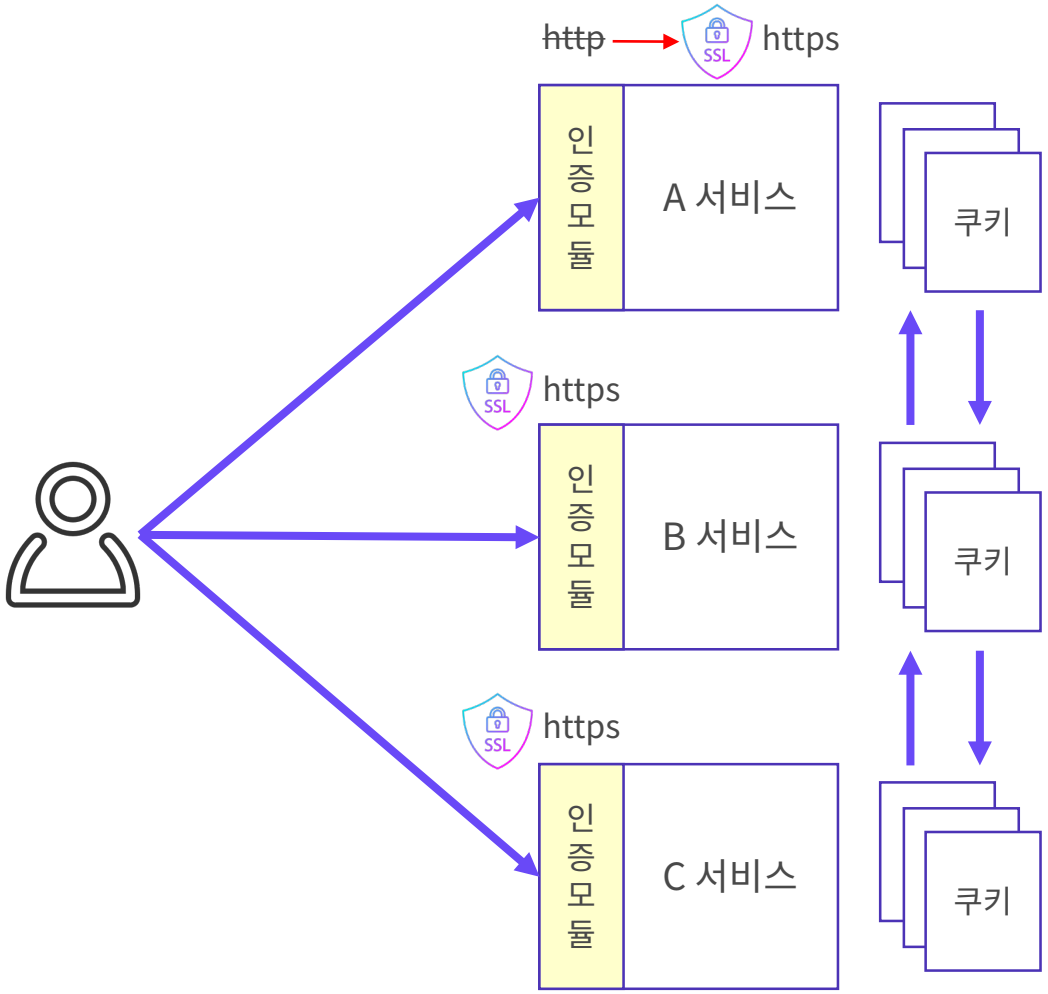
https 서비스에서의 Secure한 쿠키

이슈2: 쿠키 공유

해결방안 - 1

이슈2: 쿠키 공유

해 결 방 안 - 1



전체 서비스 SSL 적용

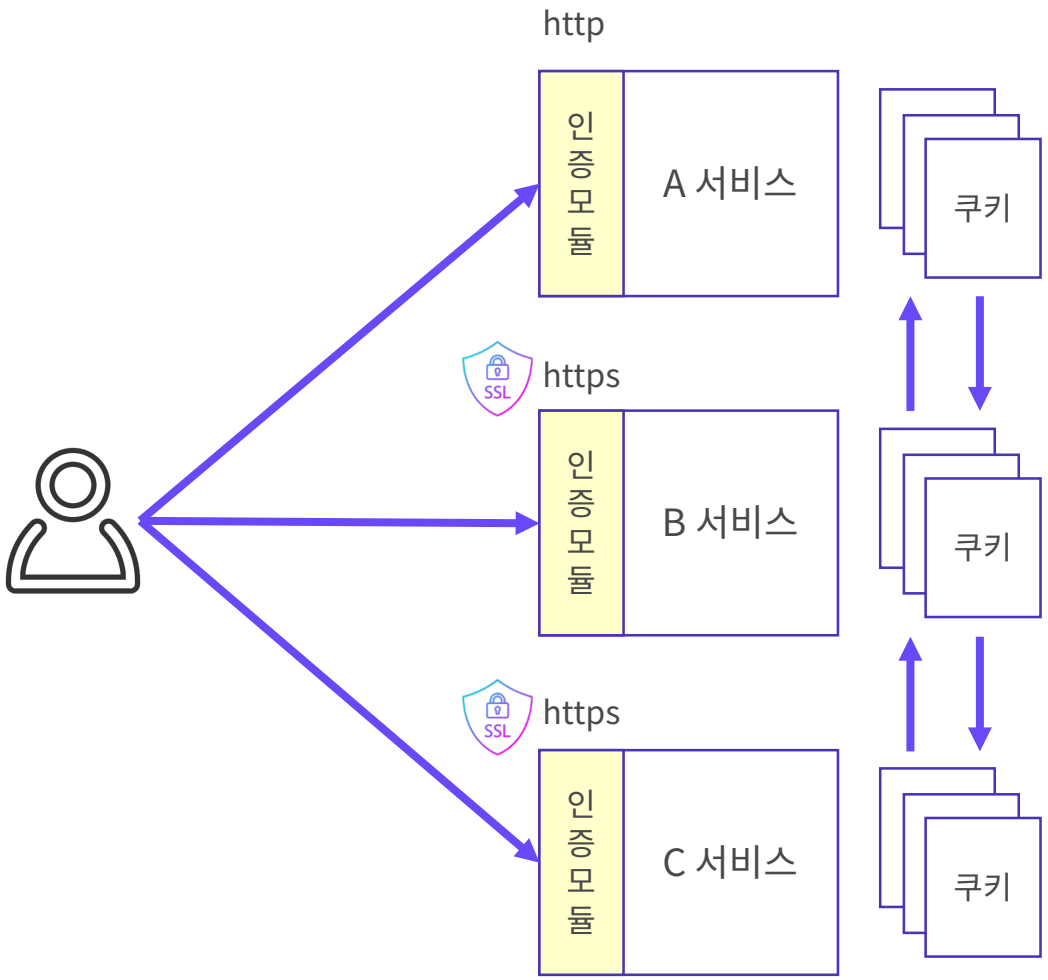
"기술적" 접근보다는 "정책적" 접근 필요

이슈2: 쿠키 공유

해결방안 - 2

이슈2: 쿠키 공유

해결방안 - 2



쿠키 생성 시 http에서의 생성

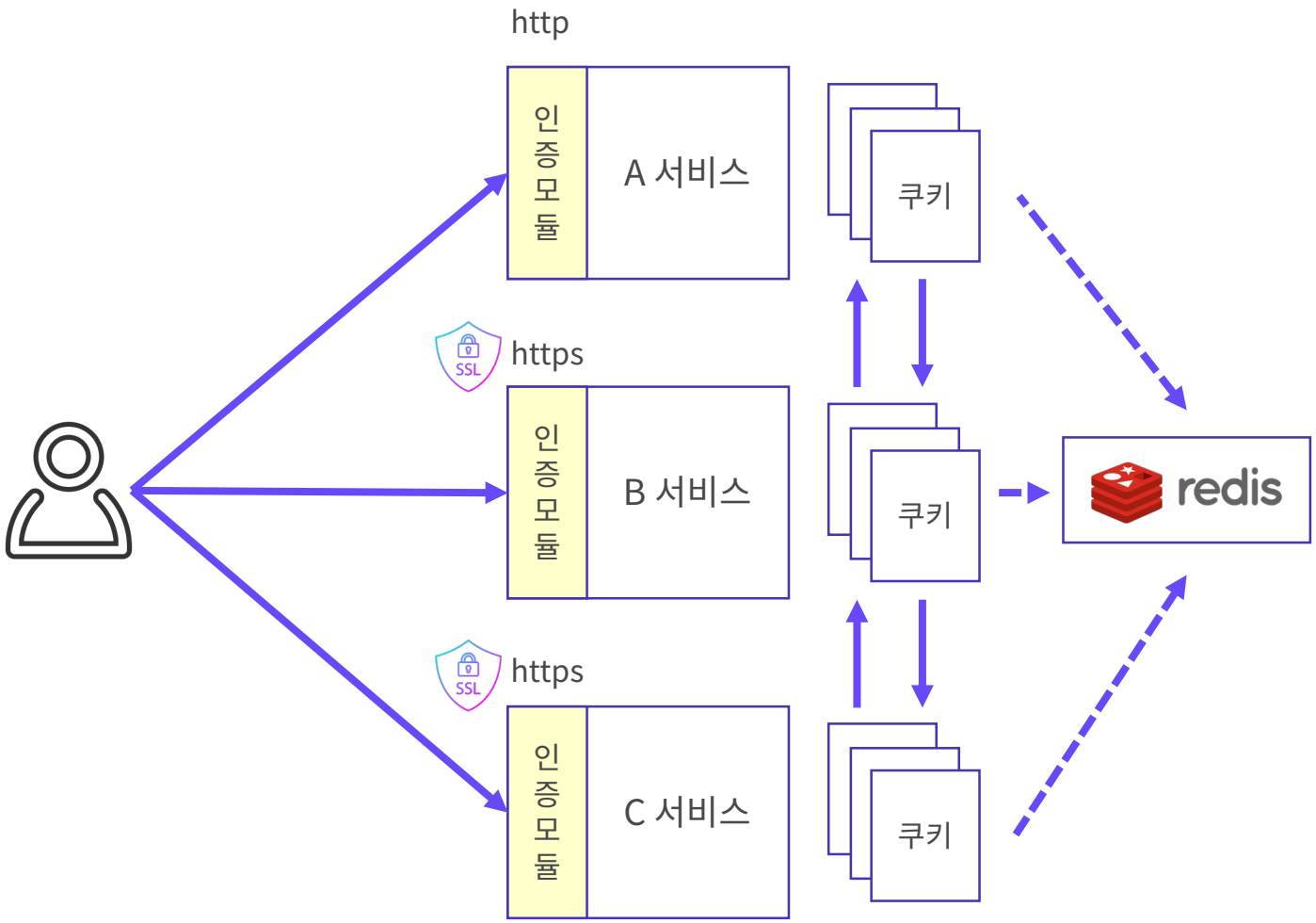
Secure하지 않기 때문에 보안에 취약

이슈2: 쿠키 공유

해결방안 - 3

이슈2: 쿠키 공유

해 결 방 안 - 3



쿠키의 대체 세션

인증 공유를 위한 redis를 적극 활용

이슈3: Legacy System의 한계

이슈3: Legacy System의 한계

전환 대상 100+

이슈3: Legacy System의 한계

전환 대상 100+

이슈3: Legacy System의 한계

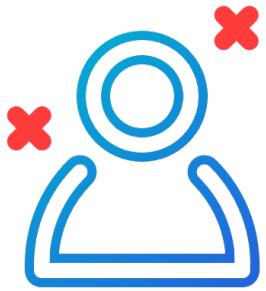
전환 대상 100+

그 중 약 30%가 Legacy System

이슈3: Legacy System의 한계

전환 대상 100+

그 중 약 30%가 Legacy System



이슈3: Legacy System의 한계

전환 대상 100+

그 중 약 30%가 Legacy System

이슈3: Legacy System의 한계

해결 완료

전환 대상 100+

그 중 약 30%가 Legacy System

이슈3: Legacy System의 한계

전환 대상 100+

그 중 약 30%가 Legacy System

구축 단계에서의 전략 수립

Legacy System 지원을 위한 추가 개발(SPI 활용)

개선 방향

인증 보안 강화

NHN FORWARD

인증 보안 강화

새로운 환경
로그인 모니터링

인증 보안 강화

NHN FORWARD

새로운 환경
로그인 모니터링

2단계 인증

인증 보안 강화

NHN FORWARD

새로운 환경
로그인 모니터링

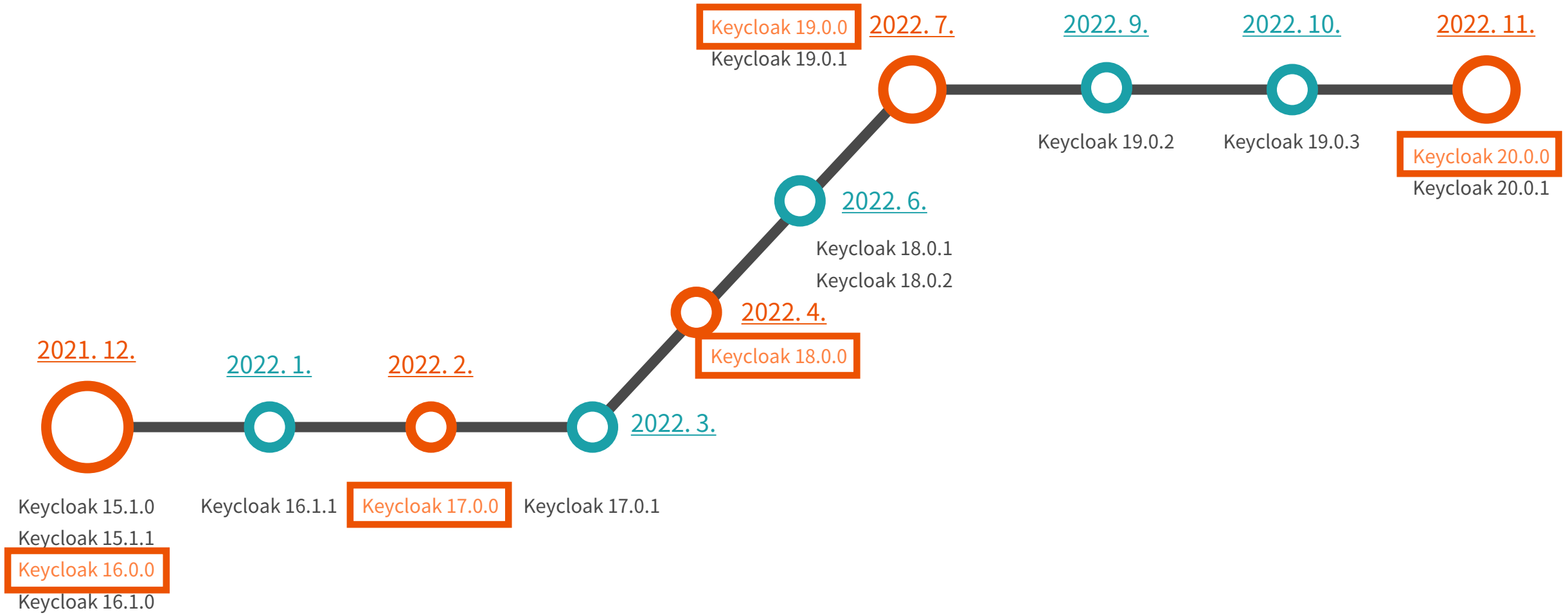
2단계 인증

인증 강제 종료

버전 업그레이드

버전 업그레이드

NHN FORWARD



버전 업그레이드는?

버전 업그레이드

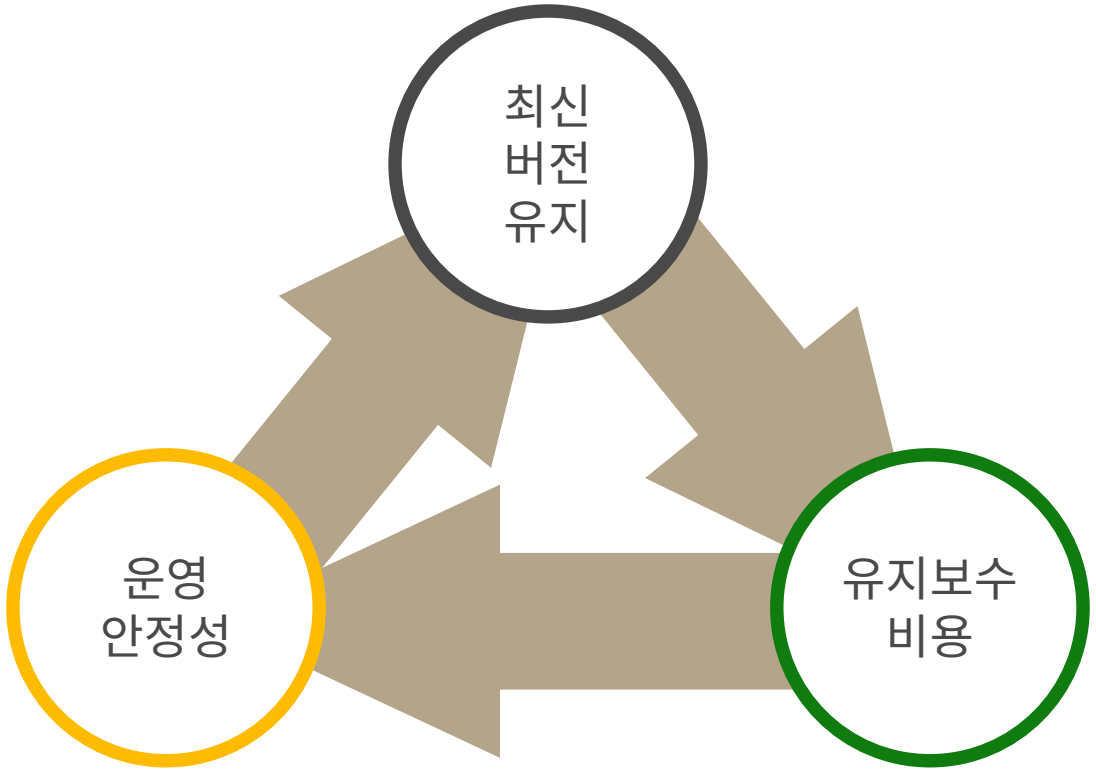
버전 업그레이드는 신중하게!

하지만, Release Note는 항상 예의주시하자.

버전 업그레이드

버전 업그레이드는 신중하게!

하지만, Release Note는 항상 예의주시하자.



그 외 여러 가지

그 외 여러 가지

- IDC 이중화
  - 대규모 장애에 대비
  - 높은 구축 비용

그 외 여러 가지

- IDC 이중화
  - 대규모 장애에 대비
  - 높은 구축 비용
- 인증 중복 체크
  - 보안 신뢰 상승
  - 외부 심사 대응(ITGC 등)

Q & A

NHN FORWARD

고맙습니다.