사용자 패스워드 변경 시 고객에 대한 유효성을 검증하는 방법은 다양합니다. 이러한 검증은 실제 계정 소유자가 맞는지 확인하고 무단 접근을 방지하는 데 중요합니다.

주요 검증 방법들:

1. **이메일 검증**
   * 패스워드 변경 링크를 사용자의 등록된 이메일로 발송
   * 일회용 확인 코드(OTP) 발송
2. **SMS/문자 인증**
   * 휴대폰으로 일회용 인증 코드 발송
   * 문자 메시지를 통한 확인 링크 제공
3. **인증 앱 활용**
   * Google Authenticator, Microsoft Authenticator 등의 앱을 통한 코드 생성
   * Push 알림을 통한 승인 요청
4. **SNS 계정 연동 인증**
   * 페이스북, 구글, 애플 등 연결된 소셜 계정을 통한 인증
   * OAuth 기반 소셜 로그인을 통한 검증
5. **생체 인증**
   * 지문, 얼굴 인식, 홍채 스캔 등 생체 정보를 통한 인증
   * 모바일 기기의 생체 인증 시스템 활용
6. **현재 비밀번호 확인**
   * 기존 비밀번호를 입력받아 검증
   * 기존 로그인 세션 확인
7. **보안 질문 확인**
   * 사전에 설정한 보안 질문에 대한 답변 검증
8. **디지털 인증서**
   * PASS 앱(한국), 공동인증서, FIDO 등을 활용한 인증
   * 디지털 서명 기반 인증
9. **하드웨어 보안 키**
   * YubiKey나 기타 U2F/FIDO2 호환 보안 키를 통한 물리적 인증
10. **위치 기반 인증**
    * 일반적으로 접속하는 위치와 일치하는지 확인
    * 의심스러운 위치에서의 접속 시 추가 검증 요구