4장. 키분배와 사용자 인증

4.6 통합신원관리

4.6 통합신원관리

- 통합신원관리(Federated identity management)
  - 상대적으로 새로운 개념
  - 다수의 기업과 많은 응용 프로그램을 관리하는 일반적 신원관리시스템
  - 수천 또는 수백만 명의 사용자를 지원하는 관리시스템

신원관리

- 신원관리(identity management)
  - 접근 권한을 가진 개인이 자원에 접근하는 절차를 중앙 집중화, 자동화하는 방법
  - 각 사용자(사람 또는 프로세스) 신원 정의, 속성과 신원 연관, 사용자가 신원을 인증하는 방법을 강요
- 싱글사인온(SSO: single sign-on)
  - 신원관리 시스템의 중심적 개념
  - 사용자가 한 번만 인증하면 네트워크 모든 자원에 접속가능

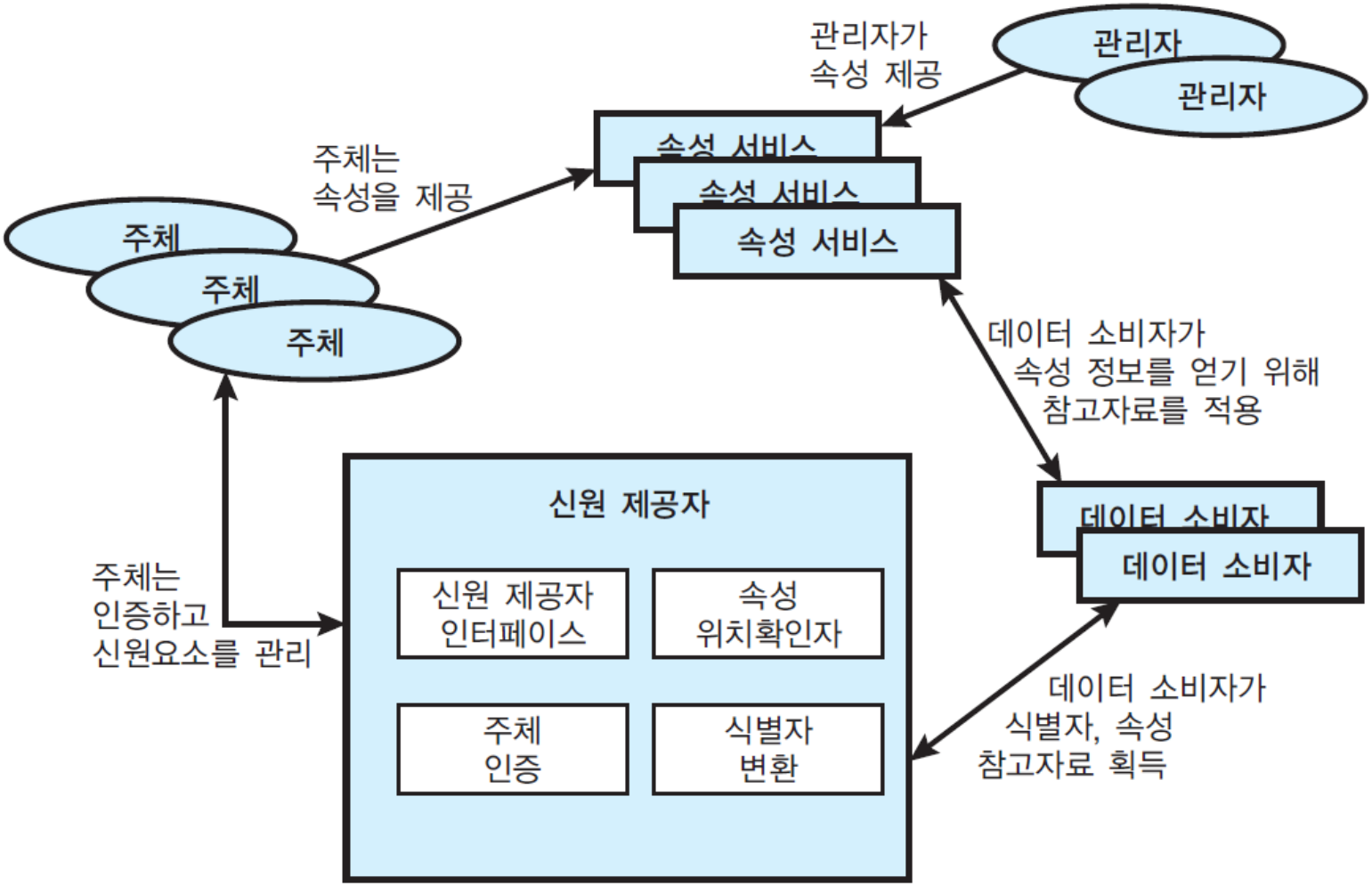
신원관리 원칙 (1)

- 인증(Authentication):
  - 제공한 사용자 이름과 사용자가 일치하는지 확인
- 허가(Authorization):
  - 특정서비스나 자원에 접근을 허락하는 일
- 계정(과금)(Accounting):
  - 로그인 접근과 허가 절차
- 제공(Provisioning):
  - 시스템에 사용자 등록
- 작업절차 자동화(Workflow automation):
- 관리 위임(Delegated administration):

신원관리 원칙 (2)

- 패스워드 동기화(Password synchronization):
  - SSO 또는 RSO(Reduced sign-on) 절차 생성
  - RSO: 여러 차례 사인온 해야 하는 번거로움은 존재, 각자의 자원과 서비스가 자체적 인증시스템으로 관리될 때 사용자가 매번 인증하는 절차를 간소화
- 셀프-서비스 패스워드 리셋(Self-service password reset):
  - 사용자가 자신의 패스워드 갱신하도록 함
- 통합(Federation):
  - 인증과 허가 절차를 한 시스템에서 다른 시스템으로 전달 (보통 여러 개의 기업 사이에서 이루어지므로 인증 절차 간소화)

일반 신원관리 구조 (1)


관리자가
속성 제공
관리자
관리자
주체는
속성을 제공
속성 서비스
속성 서비스
속성 서비스
주체
주체
주체
데이터 소비자가
속성 정보를 얻기 위해
참고자료를 적용
데이터 소비자
데이터 소비자
주체는
인증하고
신원요소를 관리
신원 제공자
신원 제공자
인터페이스
속성
위치확인자
주체
인증
식별자
변환
데이터 소비자가
식별자, 속성
참고자료 획득

일반 신원관리 구조 (2)

- 신원 소지자 (중심 개체)
  - 자원이나 서비스에 접근하고자 하는 사람(사용자 장치, 에이전트 프로세스, 서버)
  - 신원 제공자(identity provider)에게 자신을 인증
- 신원 제공자
  - 인증정보를 중심개체 뿐만 아니라 속성과 하나 이상의 식별자와 연관시킴
- 디지털 신원
  - 식별자, 인증정보(패스워드, 생체 정보), 속성(attribute)
- 속성 서비스
  - 속성 정보를 생성, 유지
- 관리자(administrator)
  - 사용자에게 역할, 접근허가, 직원정보 같은 속성 부여
- 데이터 소비자(data consumer)
  - 신원이나 속성제공자가 관리하고 제공하는 데이터를 받아 사용하는 개체
  - 허가 결정, 감사 정보 수집

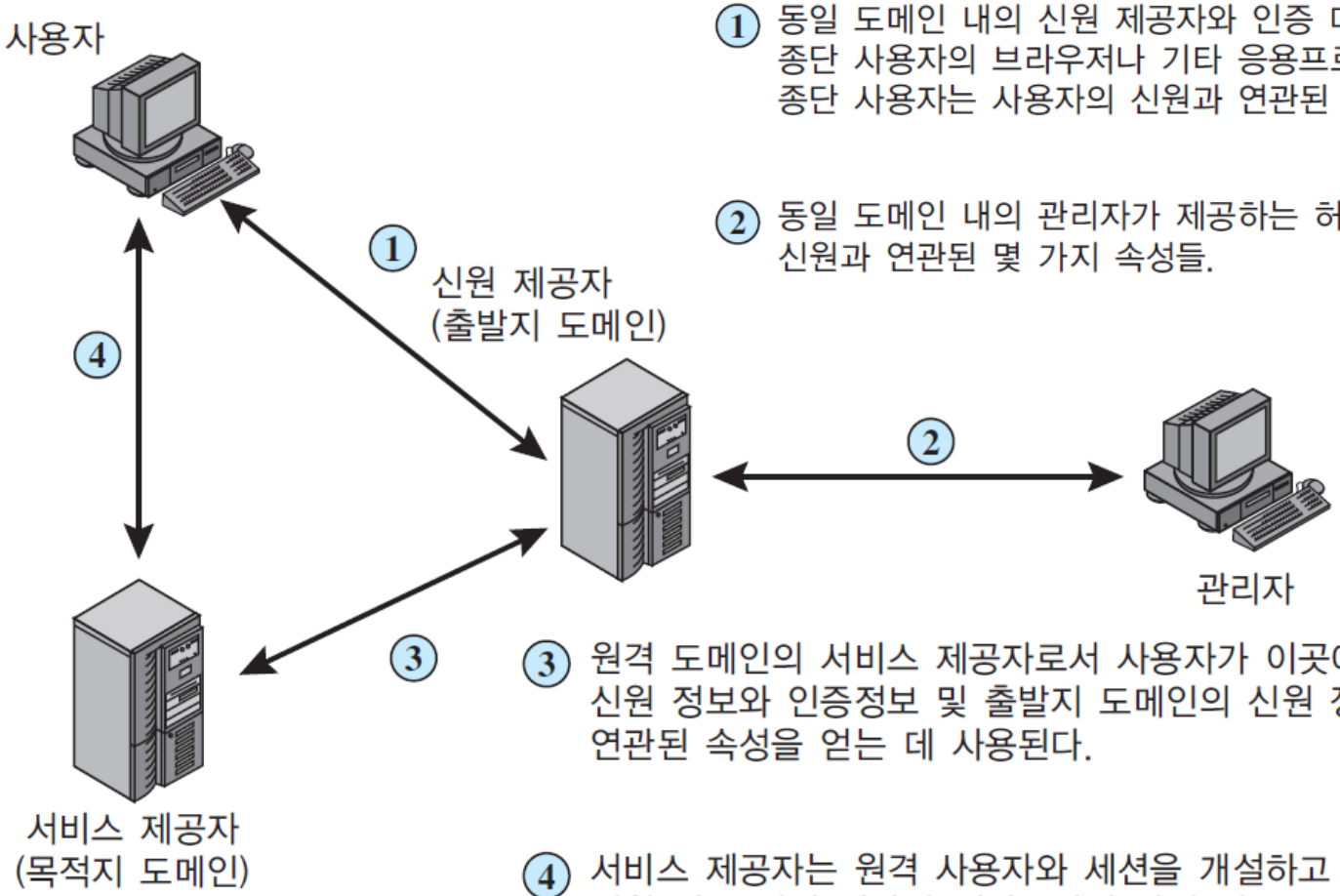
신원 통합 (1)

- 신원 통합(identity federation)
  - 다중 보안 도메인으로 확장된 신원관리
    - 자치적 내부 비즈니스 단위
    - 외부 비즈니스 파트너
    - 기타 제3자 응용 및 서비스
  - 목적
    - 디지털 신원 공유를 통해 싱글 사인온을 제공
    - 중앙집중화 된 통제가 불가능
    - 안전한 디지털 신원 공유를 위해 표준화나 상호 신뢰수준에 동의해서 통합

신원 통합 (2)

- 통합신원관리
  - 다수 기업에 신원, 신원 속성과 자격부여를 이식하고 다양한 응용 프로그램 사용을 가능하게 하며, 수천 명 또는 수백만 명의 사용자를 지원하는 합의, 표준과 기술
  - SSO
  - 속성을 나타내는 표준화된 수단 제공
  - 신원 매핑
    - 한 도메인의 사용자 신원과 속성을 다른 도메인에서 요구하는 사항에 맞추어줌

통합 신원 동작



① 동일 도메인 내의 신원 제공자와 인증 다이얼로그 시 종단 사용자의 브라우저나 기타 응용프로그램. 종단 사용자는 사용자의 신원과 연관된 속성 값을 제공.

② 동일 도메인 내의 관리자가 제공하는 허락된 역할 같은 신원과 연관된 몇 가지 속성들.

③ 원격 도메인의 서비스 제공자로서 사용자가 이곳에 접근하고, 신원 정보와 인증정보 및 출발지 도메인의 신원 정보자와 연관된 속성을 얻는 데 사용된다.

④ 서비스 제공자는 원격 사용자와 세션을 개설하고 사용자의 신원 및 속성에 기반한 제한요건에 맞춰 접근통제를 한다.

표준

- 동일하거나 서로 다른 도메인 또는 시스템에서 안전한 신원 교환을 하기 위한 조치로 다수의 표준 사용
- 조직에서는 협업 파트너가 처리할 수 있는 일종의 보안 티켓을 사용자에게 발행
- 신원 통합 표준
  - 티켓 내용과 형식을 정의하고, 티켓 교환용 프로토콜을 제공하고, 다양한 관리업무를 수행하는 것
    - 속성 전달 수행에 필요한 시스템 구성
    - 신원 매핑
    - 로그인 수행
    - 감사

SAML
(Security Assertion Markup Language)

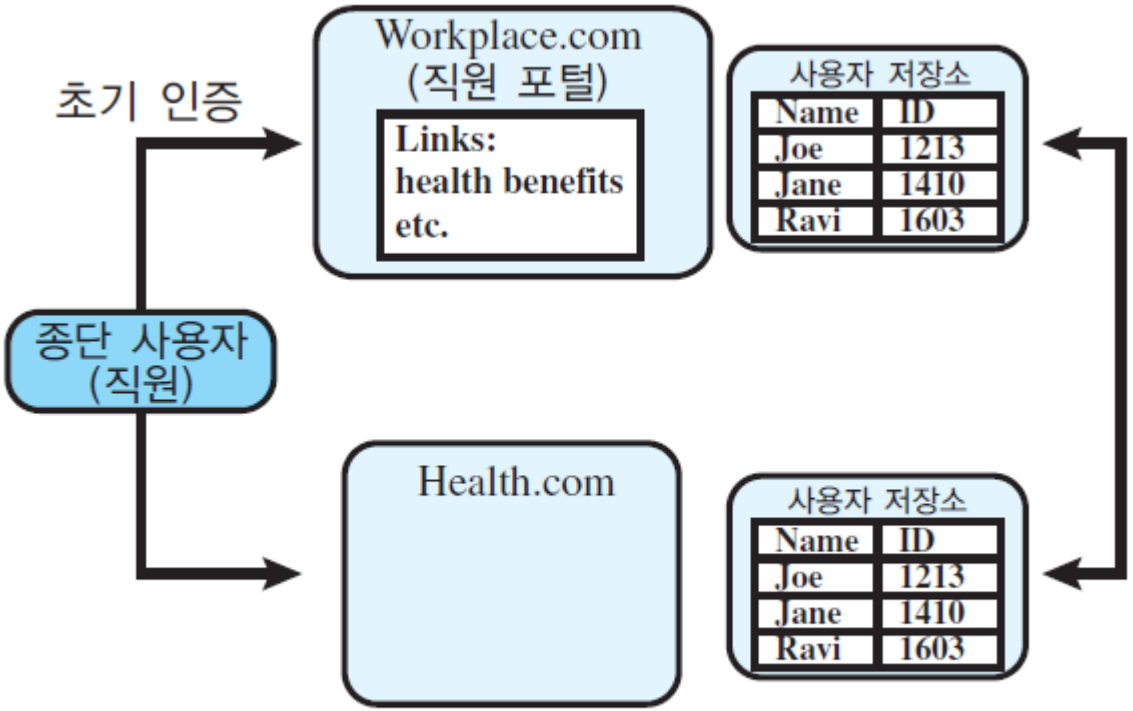
- 원론적 기본 표준
- 보안정보 교환에 대한 정의
  - 주체에 대한 주장(statement) 형식으로 전달
- OASIS(Organization for the Advancement of Structured Information Standards)가 통합신원관리용으로 발행한 광범위한 표준 집합의 일부
  - 예: WS-Federation
- 통합신원관리 구현 문제
  - 안전하고 사용자에게 편리한 유틸리티를 제공하기 위해 다수의 기술, 표준, 서비스를 집약의 어려움
  - 산업체에서 광범위하게 사용되고 있는 표준 사용

사례

- 3가지 시나리오
  - 시나리오 1
  - 시나리오 2(브라우저-기반)
  - 시나리오 3(문서-기반)

시나리오 1

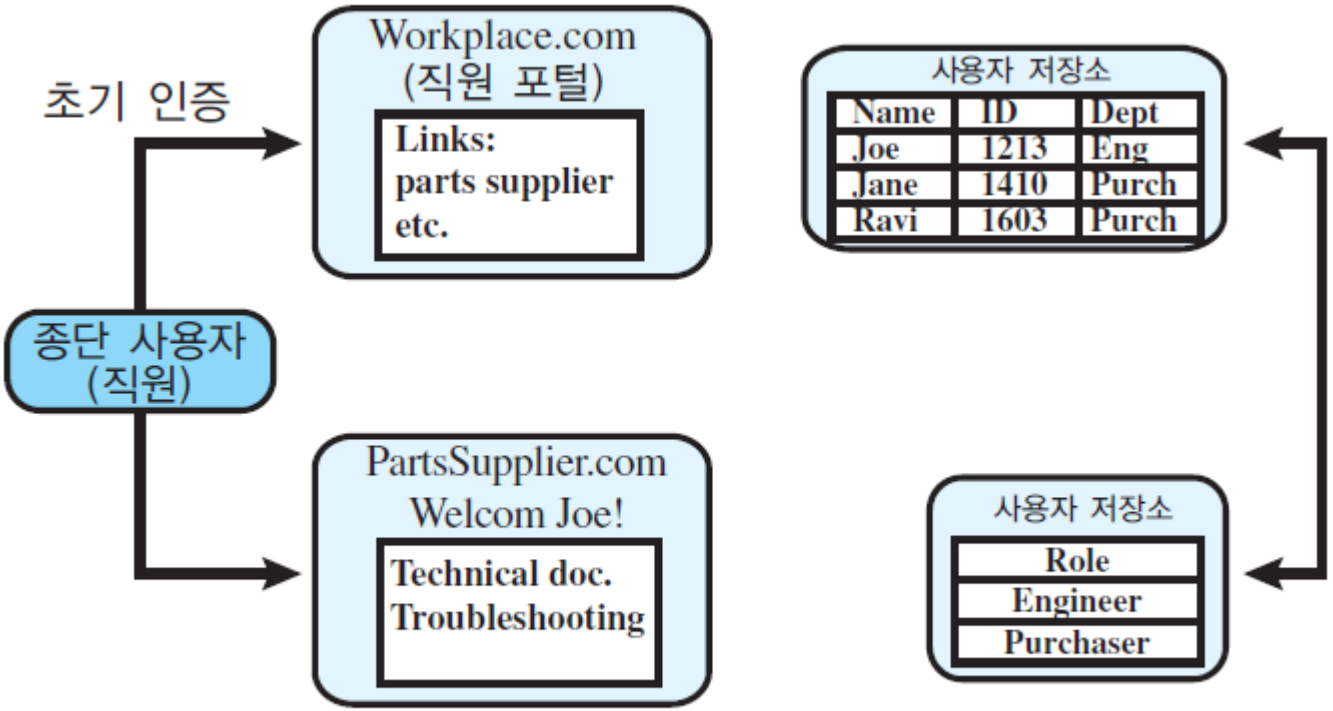
- Health.com과 맺은 Workplace.com 계약에 의해 직원은 건강 혜택을 제공받는다



(a) 계정 연결기반 통합

시나리오 2

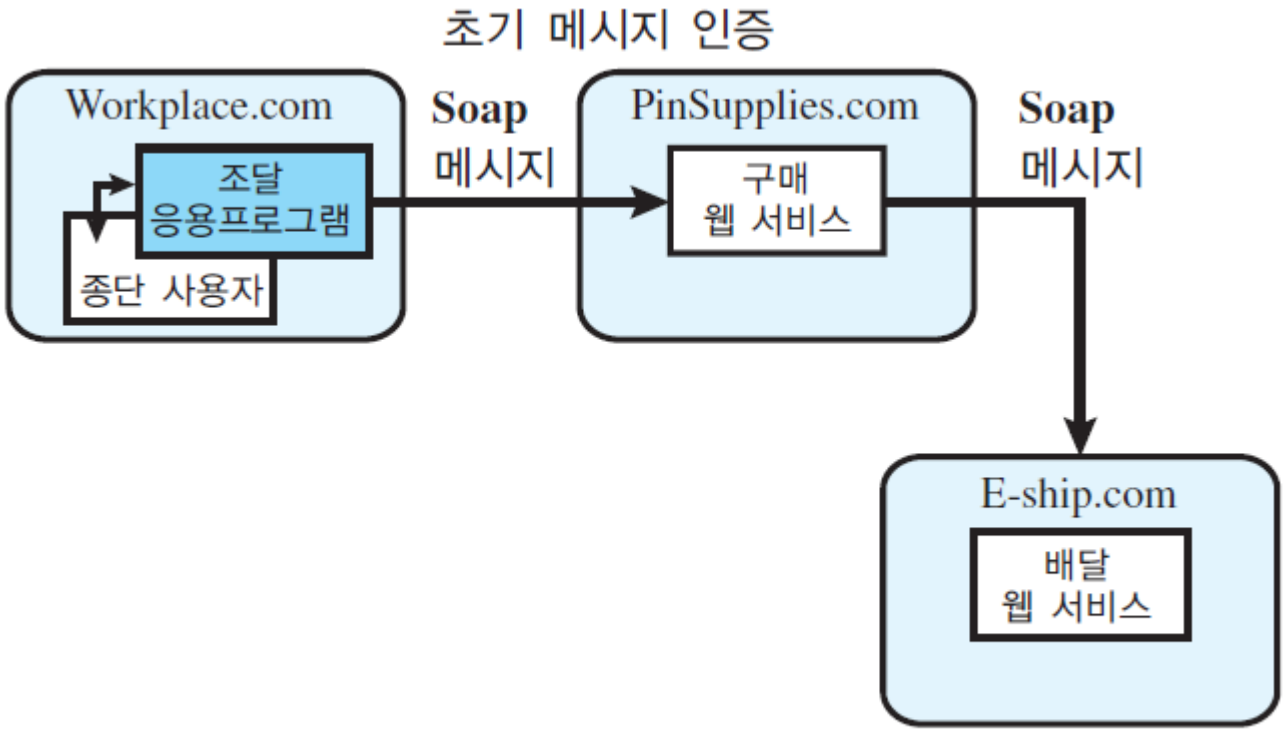
- PartsSupplier.com은 Workplace.com에 정기적으로 부품을 제공
  - 역할기반통제(RBAC)



(b) 역할 기반 통합

시나리오 3

- Workplace.com은 PinSupplies.com과 구매동의를 한 상태이고, PinSupplies.com은 E-Ship.com 사와 비즈니스 관계
  - XML/SOAP기반 메시지 작성



(c) 연쇄 웹 서비스

과제

- 복습문제 4.1, 4.3. 4.6, 4.8, 4.10, 4.13