3

상황인지 커뮤니티 컴퓨팅 환경에서의 접근제어 정책과 개인 정보 보호

충남대학교 ▌김윤삼* · 조은선**

1. 서 론

커뮤니티 컴퓨팅(Community Computing)은 사용자 주변의 사물들이 사용자의 의도를 파악하고 커뮤니티를 구성하여 협업해 나가는 컴퓨팅 방식을 일컫는다[1]. 하나의 서비스는 다수의 협력하는 개체들 간의 상호작용을 통해서 제공되며, 유비쿼터스 컴퓨팅 지능공간(USS: Ubiquitous Smart Space)처럼 환경 어디에나 컴퓨팅 기능이 존재하여 상황에 맞게 적절히 반응하는 유비쿼터스 상황인지 컴퓨팅(ubiquitous context-aware computing) 환경을 위해 사용된다.

상황을 인지하는 컴퓨팅 방식의 알려진 응용들 중 많은 부분은 개인화된 맞춤 서비스들(customized services)이라 할 수 있다[2]. 즉, 개인의 행위나 상태 데이터를 유비쿼터스 센서로부터 읽어 들인 후 최적의 반응을 찾아 서비스 하는 것이다. 이 때, 서비스를 위해 커뮤니티의 소속 개체들에게 전달되는 데이터들 중에는 민감한 개인 정보가 포함 될 수가 있으며, 이로 인하여 개인정보의 오남용이 발생할 소지가 있다. 하지만, 개인정보의 제공없이 개인화된 맞춤 서비스를 제공하는 것은 불가능하다.

따라서 상황 인지 커뮤니티 환경에서는 서비스 이용자의 개인정보 노출을 최소화 하면서 유익한 서비스를 제공할 수 있는 기능이 필수적이라 할 수 있다. 그러나 복잡하고 동적인 시스템의 특성상, 기존의 정보보호 기법이나 개인 정보보호 기법 외의 특화된 해결법이 요구되고 있다.

본고에서는 다양한 유비쿼터스 상황인지 커뮤니티 컴퓨팅에서 요구되는 정보보호 기법의 동향을 가장 주요한 측면 중 하나인 접근 제어 기술을 중심으로 정리하고, 이와 관련하여 상황 인지 컴퓨팅에서의 개인의 정보 유출에 대한 기술 동향을 다루었다. 2장과 3장에서는 유비쿼터스 컴퓨팅의 특성상 고려할 필요성이 있는 상황 정보의 보호와 상황과 관련한 정책의 운용 등으로 확장되어 연구되고 있는 부분을 각각 정리하였다. 4장에서는 이와 관련하여 상황 인지 컴퓨팅에서 개인 정보 보호를 위한 기법들 중 정보 누출, 클러킹(cloaking), 익명성 등에 대해 다룬다.

2. 상황 정보에 대한 보호

상황 정보는 단위 정보들이 상호 관계를 이루고 있다는 점과 이동 정보를 비롯한 동적인 정보를 포함하고 있다는 점에서 고전적인 정보들과 차이를 가진다.

간단한 경우에는 관계형 데이터 모델, XML 등으로 표현될 수 있는데, 일반적인 관계형 또는 XML 데이터베이스 시스템의 접근제어에 대한 연구 결과[3,4]를 그대로 적용하게 된다.

특히 단위 정보가 서로 네트워크된 상황 데이터는 시멘틱웹 표현 방법에 의해 기술하는 것이 적합하다. W3C의 RDF(Resource Description Framework), OWL(Web Ontology Language)등이 그 예이다. 이를 위하여 RDF나 OWL의 접근제어에 대한 연구 결과를 응용할 필요가 있는데, 대부분의 연구가 최근에 이루어지고 있다.

RDF에 대한 접근제어 방법 역시 기존의 접근제어 정책과 같이 단위 데이터에 대해 접근 권한을 명시해야한다. 미 Maryland 대에서 개발한 RAP(RDF Access-control Policies)[5]은 RDF의 기본 데이터 단위인 트리플(triple) 즉, 〈subject, property, object〉에 대해 접근 제어하는 것에 초점을 두고 있다. 특히, RDF 트리플의 각 원소에 와일드카드를 사용한 '트리플 패턴(triple pattern)'을 질의와 연산에서 사용할 수 있도록 하여 논리 언어에 기반 하여 정책을 정의하면 동시에

* 학생회원
** 종신회원
† 본 연구는 21세기 프론티어 연구개발사업의 일환으로 추진되고 있는 지식경제부의 유비쿼터스컴퓨팅및네트워크원천기반기술 개발사업의 09C1-T3-10M 과제로 지원된 것임

```
permit(update(A,(P, emp:salrary,?),
  (P, emp:salary,?)) :- b
      existTriple(A, emp:Supervisor, P)
```

그림 1 RAP 접근 정책의 예[5]

많은 데이터에 대한 접근제어 정책 정의가 가능하다. 그림 1은 어떤 사람의 상사(supervisor)는 그 사람의 월급을 열람할 수 있다는 내용의 정책이다.

온톨로지 데이터의 추론을 고려한 접근 제어 정책 정의에 대한 연구도 필요하다. 먼저, 추론 자체가 정보 유출을 야기할 수도 있어 이에 대비해야하므로, 추론된 데이터에 대해 접근제어 정책이 원본 데이터의 접근 제어 정책으로부터 자동으로 설정되도록 정의할 수 있다. 그러나 특정 데이터가 추론에 의해 접근되는 경우와 그렇지 않고 직접 접근되는 경우의 정책들이 각각 다를 수가 있다는 문제가 있다. RACL(RDF access control language)은 이와 같은 상황을 정책의 충돌(conflict)로 간주하고 해결하고자 노력하였다[6]. 여기서는 앞서 소개한 트리플 패턴을 사용하여 접근제어의 대상 정보를 정의하는 구조를 가지므로 추론이 없더라도 서로 다른 두 정책이 적용될 가능성이 있는데, 이 경우는 보다 구체적으로 묘사된 트리플 패턴에 대한 정책이 우선순위를 가진다. 또한, RDF의 서브클래스 등의 포함관계 반영을 위한 추론 기능인 W3C RDF/S Entailment Rules[7]에 대해 접근 권한도 함께 전이되므로, 저장되어 있는 정보가 추론으로도 도출된다면, 정의된 접근 제어 정책과 전이된 접근 제어 정책이 다를 경우 서로 충돌이 일어나게 된다. 이에 대한 해결책이 되는 메타 규칙은 추론된 접근 권한이 원래의 접근 권한보다 더 제한적일 때 경고를 주는 방식이다.

보다 다양한 추론이 지원되는 OWL에 대해서는 동치(equivalent)거나, 부분(part-of)이거나, 서브클래스(subclass) 관계 등 몇 가지를 '추론 가능한 관계(inferable relation)'로 설정하고, 이 관계를 따르는 경우에는 하나의 개체에 대한 접근 권한이 전이되는 것에 대해 면밀히 정의한 연구가 있었다[8]. 정보의 단위를 컨셉이라고 하고, 만약 추론 관계가 강한(strong) 추론 관계인 경우 추론된 컨셉은 추론한 컨셉의 접근이 허용된 권한에 대하여 추가적인 접근 허용을 하게 되며, 반대의 경우에는 추론된 컨셉에 대하여 접근이 금지된 권한은 추론한 컨셉에 대하여서도 마찬가지로 접근을 금지 시킨다. 약한 추론(weak) 은 part/whole관계처럼 추론한 컨셉이 추론된 컨셉에 대하여 추가적인 권한 설정에 대한 영향을 미치지는 못하나, 반대의 경우에는 접근 금지 항목에 대하여 영향을 미치게 된다. RDF의 경우와 마찬가지로 정책의 충돌이 발생 가능하므로 이 경우는 제한적인 권한으로 정의하게 된다.

3. 상황 정보에 의한 정책의 정의 및 운용

상황 인지 시스템에서의 접근 제어는 앞서 살펴보았듯이 상황 정보를 보호해야하는 부분도 있지만, 상황 정보가 정책 정의에 사용될 수가 있다는 점이 특징이다. 그리고 상황 인지 시스템의 동적인 특성에 의해 일반적인 접근제어 시스템과 다르게 운영되어야할 필요가 있다는 점도 가지고 있다.

3.1 상황이 내재된 접근 제어 정책

접근 제어란 누구(who)에게 데이터(what)의 무슨 작업(how)을 하는 것을 허용할 것인지를 정책으로 미리 정의해 두고 이에 따라 접근의 허용/불허를 정의하는 것이다. 이러한 일반적인 접근제어와 달리 상황 정보에 따른 접근 제어는 장소(where), 시간(when), 목적(why) 등의 상황 정보가 접근 허용에 대한 조건에 이용되게 된다. 대표적으로 미 카네기멜론 대의 AURA[9]는 그림 2와 같이 장소(Wean홀, Doherty홀의 1234호), 시간(월요일 8시부터 12시, 화요일 13시부터 14시) 등 상황 정보로 표현된 조건을 기술하고 있다.

미 매릴랜드 대학의 Rei[10]는 접근 제어 뿐 아니라 상황 인지 시스템 전반에서 사용될 수 있는 정책 정의 언어로서, W3C의 온톨로지 표준화 작업인 SOUPA[11] 중 정책 분야의 표준안의 기초가 된 것으로 알려져 있다. Rei로 정의된 정책은 허용(right)/불허(prohibition)만을 기술하는 일반 접근 제어 정책 언어와는 달리, '반드시 해야함(obligation)', '더 안 해도 좋음(dispensation)' 등의 Deontic 로직에 대한 정의도 포함할 수 있어, 접근제어 뿐 아니라 커뮤니티 개체들

```
(cert
  (issuer (public key of alice))
  (subject (public key of bob))
  (tag (policy alice
         (* set (* prefix world.cmu.wean)
                  world.cmu.doherty.room1234)
         (* set
               (monday (* range numeric
                  ge #0800# le #1200#))
               (tuesday (* range numeric
                  ge #1300# le #1400)))
               coarse-grained)
                )
       )
```

그림 2 AURA의 접근제어 정책 예[9]

```
has(john, right(nond( seq( printBW,
   repetition(printColor)), once(faxBW)),
   lab-member(john,'AI')))
```

그림 3 Rei의 접근 제어 정책 예[11]

이가지는 일반 정책으로도 사용할 수 있다. 그림 3은 'john'에게 허용된 권한을 정의한 것인데 'AI' 연구실의 일원일 경우에 한해서, 흑백 출력 후 반복적인 컬러 출력을 하거나 한 번의 팩스 사용이 가능함을 뜻한다. nond는 두개의 인자를 가지는 연산자로서 둘 중 하나를 허용한다는 의미이며 둘 모두를 허용하지는 않는다.

이 후에 등장한 상황 인지 시스템에서 지원되는 접근 제어 정책들도 주로 이와 같은 내용들을 정책에 반영하고 있다. 이러한 종류의 상황 인지 시스템의 접근제어가 특히 가장 많이 사용되는 역할 기반 접근제어와 결합한 것을 CA-RBAC(Context-AwareRole-Based Access Control)[12] 또는 CRBAC(Context-Role Based Access Control)[13] 등으로 불리는데, RBAC(Role Based Access Control) 시스템을 운영하는 데에 있어서 상황 정보에 대해 조건화하여 검증하는 과정을 포함시킨 것이다. 그리고 이러한 조건들은 경우에 따라서는 활성화/비활성화의 옵션에 의해 융통성 있게 적용되기도 한다. 예를 들어 유비쿼터스 시스템의 유용한 응용인 u-헬스 분야나 긴급 구호 상황 등에는 필수적인 기능으로 볼 수 있다[14].

3.2 상황 인지 정책의 운영

상황을 고려한 정책의 운영에서, 상황 정보는 인증 시점과 접근 및 권한 도출 시점에 주로 참고 되고 있다. 그러나 상황 인지 시스템에서는 이 외에도 상황정보가 변화될 때 등 다양한 시점에 정책을 재검증할 필요가 있다. 미 MIT대학의 인자화된 정책(parameterized policy)[15]은 OWL 온톨로지 데이터 기반의 상황정보에 대해 OWL 규칙으로 접근제어 시스템을 구성한 것으로서, 상황 정보를 정책의 인자로 간주하는 접근제어 정책을 가지고 있다. 결과적으로 상황에 따라 다른 규칙을 적용하도록 구성되는데, 이는 원칙적으로 상황 정보가 바뀌면 정책 자체가 바뀌는 것을 의미하고 있어 어떠한 시점에서 검증을 하더라도 변경된 상황 조건을 반영할 수 있도록 한다.

이에 더 나아가 이미 허용된 내용에 대해서도 조건의 진리값 변화에 따라 부적합한 상황으로 바뀔 수 있는 점을 고려할 필요가 있다. 공용 장소의 공유 장치에 대한 접근제어는 더더욱 이러한 점이 필요한데, 미 캘리포니아 대에서는 사용기간이 긴 장비에 대해, 특히 여러 장비를 동시에 로그인해서 사용하는 경우[16], 요청했던 당사자가 계속 사용하고 있는지에 대해 검증하는 보다 철저한 프로토콜을 제안하고 있다.

3.3 장비에 대한 고려

상황인지 커뮤니티 컴퓨팅에서는 사용자 주변 상황을 인지하기 위해 일반적인 응용들과는 달리 다양한 센서 및 액츄에이터 장비들을 연동시킨다. 이러한 장비들로 인한 특성을 접근 제어 정책에서 고려할 필요가 있다.

먼저 장비가 인지해 내는 상황의 불확실성에 대한 특성을 정책에 반영하기도 한다. 미 일리노이 대학의 상황 인지 시스템인 GAIA의 보안시스템 Ceberus[17]는 인증 장비마다 확실성(confidence) 레벨을 부여하고, 이를 정책에서 활용하고 있다. 그림 4는 스마트시계는 70%, 스마트 뱃지는 10%, 지문스캔은 90% 등의 확실성 레벨을 부여된 상태에서, 확실성이 60% 이상인 경우에만 컬러프린터를 접근 할 수 있다는 정책이다.

장비들의 사용에 대한 제어도 접근 제어 시스템이 다루어야할 영역중 하나이다. 미 미네소타 대학에서는 특정 세션동안 특정인에게 동적으로 지정된 장비에 대한 권한을 정의하는 방안을 도입했다[12]. 기본적으로는 역할 기반 시스템을 견지하고 있으나, 다른 역할 기반 시스템과 달리, 역할(role)이 동일하다 하더라도 권한이 각 구성원에 특화되어 달라질 수 있도록 하는 '개인화된 권한(personalized permission)'을 지원하고 있다. 동일 역할에 속하는 구성원 간에 공유되는 데이터와 공유될 수 없는 데이터를 '공유 개체(shared object)'와 '개인적 개체(private object)'로 각각 명명하고 있다. 또한 이 시스템은 역할의 정의 내부에 해당 역할이 수행해야하는 작업들을 함께 기술하여 응용 프로그램을 작성하게 되는 것이 특징인데, 개인적 개체도 역할의 정의 내에 기술되도록 함으로써 공유 개체와 구분한다. 그림 5는 역할 Nurse의 구성원에 특화된 개인적 개체 MyPrinter가 개인적 개체임을 나타낸다. 이것은 동적으로 바인딩 되어 특정 세션동안 특정 간호사에게 바인딩 된다.

```
ConfidenceLevel (smart_watch, 70%)
ConfidenceLevel (smart_badge, 10%)
ConfidenceLevel (fingerprint_scan, 90%)
CanAccess(P, ColorPrinter) := ∃number V
  (ConfidenceValue(P,V) ∧ V>60%)
```

그림 4 Ceberus의 접근제어 예[17]

```
Role Nurse {
  Object MyPrinter RDD (...) {
                // 개인적 개체 (Private Object)
      Reaction {... }   // 바인딩 관련
  }
  Operation Print {
      Action MyPrinter SessionMethod print
  }
}
```

그림 5 CSAC의 개인화된 권한의 예[12]

3.4 상황 인지 인증

접근제어 정책은 사용자가 누구인지 이미 인증 되었다는 가정을 하고 시작된다. 이러한 인증은 사용자의 태그나 뱃지, 신분증 또는 생체적 방식을 통해 이루어지며 인증 과정 자체는 사용자의 명시적 개입이 요구된다.

상황 민감 접근 제어(Context-Sensitive Access Control, SCAC)[17]에서는 유비쿼터스 컴퓨팅의 기본 철학에 충실하도록 인증 시 사용자의 개입 없이 상황정보를 보고 주체를 판단한다. 즉 CA-RBAC이나 CRBAC이 인증에 의해 파악된 역할(role)과 상황정보를 가지고 권한을 판단한다면, SCAC는 인증 없이 상황 정보만을 정보 요구 주체를 판단하는 방법이다. 오류가 많이 발생할 수 있다는 단점을 가지고 있지만, 신뢰도가 높은 타 개체의 소개인지 확인하거나, 위치 정보인 경우 근처에서 확인하거나, 상황의 이력을 추적하여 개연성을 확인하거나, 다른 검증된 개체와의 행동이 비슷한지 비교하는 방법을 통해 보완하게 된다.

4. 개인화된 서비스와 정보 보호

개인화된 서비스(customized service)의 증가에 의해 개인정보의 보호가 중요한 이슈가 되었다. 여기서는 앞서 살펴본 상황인지 시스템에서의 개인 상황 정보 보호에 관련된 주제들을 다루고자 한다.

먼저 유비쿼터스 상황 정보 시스템에서의 정보 누출 모델에 대해 살펴보고, 기존의 접근 제어 기법을 확장하여 유용한 개인화 서비스의 접근 불허를 감소시키는 '클러킹(cloaking)'을 중심으로 이에 대한 해법을 정리하였다.

4.1 상황인지 시스템의 정보 누출(leakage) 모델

상황을 인지하여 작업을 수행하는 시스템에서의 데이터 누출은 상황 정보의 특성상 기존의 여타 성격의 정보 누출과 다른 측면을 가지고 있다.

미 카네기멜론대의 연구에서는 상황정보에 의해 조건화된 접근 제어 정책 운영이 정보 누출을 야기할 수 있다는 점을 들고, 다음 세 가지 가능성을 예로써 제시하고 있다[2]. 먼저, (1) Alice가 자신의 일정을 자신의 사무실 문 앞에서 기다리는 사람에게만 허용한다고 했을 때 Bob이 Alice의 일정을 질의하는 경우 Bob의 위치를 Alice나 일정 서비스 쪽에 누출 시킬 가능성이 있다. (2) 또한 Alice가 자신이 사무실에 있을 때만 자신의 일정을 허용한다고 할 때, Alice가 사무실에 있는지 여부가 정보를 접근하는 사용자들에게 노출되게 된다. (3) 보다 의도적인 경우에는 Bob이 특정 위치에 있을 때만 Alice의 일정을 Alice 자신에게 공개하도록 하는 비상식적인 정책을 정의함으로써, Alice가 Bob의 위치를 알아내도록 지정할 수도 있다. 카네기멜론 대학에서는 조건화된 상황정보를 정책에 관여된 주체나 서비스들에게 감춤으로써 이를 해결하는 기법을 제시하고 '은닉된 조건(hidden constraint)'이라고 명명하고 있다. 또한 특정 정책을 집행할 때에는 조건부에 명시되어 있는 상황에 대한 접근 권한을 반드시 가져야하는 신뢰 시스템의 기반 구조를 제시하였다.

상황 인지 시스템의 특성 중 다양한 장치들이 연동되어 센싱하거나 동작하는 것을 이용한 누출도 가능하다. 장비의 동작을 물리적으로 목격될 수 있으므로 경우에 따라서는 보유 정보와 목격된 동작으로 상황정보를 유추할 가능성도 있다. 이탈리아 밀라노 대학[2]에서는, 유비쿼터스 운동 센터에서 제공되는 운동 추천 서비스가 〈성별, 나이, 신체데이터(지수)〉를 가지고 결정되는 경우 정보 누출이 일어날 수 있다고 지적하고 있다. 즉, 취득한 성별과 나이 정보만으로는 요청자가 누구인지 알 수 없지만, 추천한 운동을 하고 있는 사람을 관찰할 수 있으므로 이를 토대로 알아낼 수 있고, 결국 자신의 회원 정보와 맞추어 보면 〈요청자, 요청자의 신체 데이터〉 쌍이 얻어지게 될 것이라는 점이다. 이들은 보편적인 익명화와 더불어, 다음 절 이후 소개될 '클러킹(cloaking)' 기법을 통해 해결할 수 있다. 또한 운동 추천 시 다수의 운동을 추천하도록 하고, 익명도 레벨도 함께 제공함으로써 서비스 요청자 본인이 자신의 데이터를 보호할 수 있는 방향으로 선택을 할 수 있도록 필요한 정보를 제공할 것을 제안하고 있다.

4.2 위치 정보의 클러킹

클러킹(cloaking)[18]은 정보를 공개 할 때 상위 정보를 공개함으로써 정보를 은닉하는 기법이다. 계층적 관계를 가지는 성격의 데이터에 쉽게 도입될 수 있는

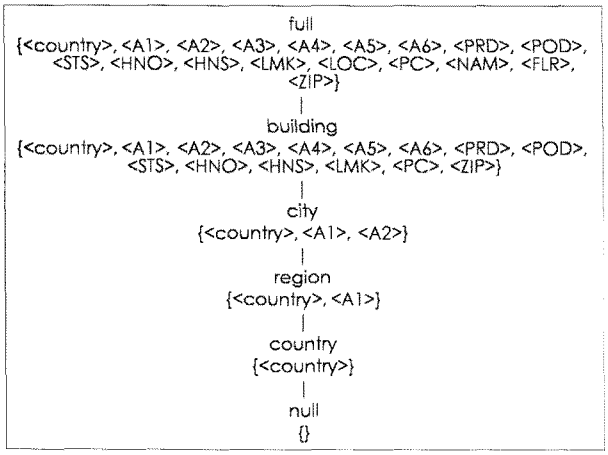


그림 6 GeoPriv 위치 정보 포맷[19]

데, 예를 들어 위치정보의 경우, "'광화문'에 있다"는 사실 대신 상위 정보인 "'서울'에 있다"는 정보를 대신 제공함으로써 밝혀지는 정보의 정확도를 감소시키고 이로써 정보의 노출 수위를 조절하는 것이다.

IETF의 워킹그룹인 GeoPriv[19]는 위치 데이터의 포맷과 이에 따른 개인 정보보호 정책 표현에 대한 표준화를 다각도로 진행해오고 있다. 그림 6은 정보의 구체성으로 구성된 GeoPriv 계층 구조를 나타내고 있다. 가장 많이 노출하는 'full' 단계의 경우는 〈country〉, 〈A1〉~〈A6〉, 〈PRD〉, 〈POD〉, 〈STS〉, 〈HNO〉, 〈HNS〉, 〈LMK〉, 〈LOC〉, 〈PC〉, 〈NAM〉, 〈FLR〉의 모든 XML 태그에 의해 명시되는 정보를 노출하고 있고, 'building', 'city', 'region' 순으로 노출 정도가 작아지면서 'country' 단계에서는 나라 이름에 대한 접근만을 허용할 수 있도록 하는 방식이다.

4.3 비정형 데이터의 클러킹

앞서 위치 정보에 대해 적용했던 클러킹은 다른 정보보호 기법에 비해 서비스의 지속성을 유지할 수 있다는 장점이 있다. 즉, 자신의 자세한 위치 정보(예, '광화문')를 공개하기를 꺼려하는 사용자가 언어 번역 서비스를 필요로 한다면 좀 더 추상적인 정보(예, '대한민국')을 공개함으로써 정보도 보호하고 서비스의 지속성도 가질 수 있다.

따라서 이러한 클러킹 기법은 위치 정보 외의 정보에 대해서도 적용시키려는 노력이 있어왔다. 예를 들어 P3P-Preference Exchange Language 1.0[20]에는 URI등에 대해 헤더 정보를 축약하는 방법을 제시하고 있다.

상황 정보에 대해서도 클러킹을 적용한 사례가 있다. 태그 기반 상황정보 접근 제어 기법[21]은 네트워킹 되어 있는 비정형 데이터 모델의 단위 데이터에 사용 목적을 나타내는 태그를 붙여 특정 목적으로 접근하는 사용자에 대해서는 허용하도록 하는 기법을 사용하여, 허용/불허로 이분하지 않고, 사용자의 목적에 맞게 추출한 데이터를 제공하는 방법을 소개하고 있다. Semantic e-Wallet[22]은 실제 데이터 대신 추상화된 버전이나 가짜 버전을 제시할 수 있도록 정책을 정의할 수 있도록 한다.

CMS[23]는 일차논리식으로 정의된 상황 정보의 추상화 수위를 미리 정의된 계층 구조에 따라서 사용자에 맞게 조정할 수 있는 기능을 취하고 있다. 계층 구조는 타입 계층 구조와 개체 계층 구조를 지원하고 있으며, Bob에게 1번째 레벨까지만 Activity와 Place 정보를 공개하겠다는 정책은 그림 7과 같이 정의된다.

```
granurarity_pref =
        when requester = Bob
        on Activity, Place
        limit level 1
```

그림 7 CMS의 접근제어 정책 예[23]

4.4 익명성과 클러킹

k-익명성(k-anonymity)은 개인 정보보호를 위한 주요한 방식으로써, 개인의 민감한 정보가 다른 k-1명의 동일한 정보를 가지는 사용자들이 존재할 때만 제공하는 것을 의미하며, 외부로 공개되는 데이터의 집합에 대하여 여러 가지 조합 또는 배경 지식을 통해 개인 정보가 노출되는 것을 막도록 하는, 이다. 만일 원본 데이터가 이러한 성질을 만족시키지 못한다면, 개인정보가 될 수 있는 데이터를 일반화(generalization)시켜 같은 정보를 가진 튜플을 만들어 제공함으로써 인위적으로 지원하기도 한다. 현재 유비쿼터스 상황인지 시스템 전반에서 이러한 익명성에 대한 중요성이 인식되고 있다[24].

앞서 소개된 클러킹과 k-익명성 지원을 함께 사용하여 익명도를 높이는 방법들도 연구되고 있다. 아직 많이 이루어진 것은 아니지만, k-익명성의 일반화와 클러킹의 계층 구조의 공통점은 이러한 연구를 가속화 시키고 있다.

만일 위치 클러킹을 익명성과 결합시킨다면, 같은 위치에 있는 사용자가 k명 이상 발생하도록, 제공되는 위치 정보를 넓게 추상화 시키는 것이다. 예를 들어 ([0,1], [0,1]) 구간에는 3인이 있고, ([1,2], [0,1]) 구간에는 3인이 있고, ([0,1], [1,2]) 구간에는 3인 ([1,2], [1,2])구간에는 1인이 존재한다고 가정한다면, k가 3일 때 3인이 존재하는 구간의 사용자들은 자신의 위치를 정확히 제공해도 k-익명성이 보장되지만, 2인이

나 1인이 존재하는 구간의 사용자들은 그렇지 않다. 따라서 익명성을 보장하기 위해 옆구간과 결합하여 (예를 들어 [0,2], [0,2] 등) 더 넓은 영역을 위치정보로 제공함으로써 익명성을 보장하게 된다. 이때의 더 넓은 영역으로 확대해서 제공하는 경우 클라킹에서 정의한 계층 구조를 사용하게 된다[25].

그러나 이 방법은 구간이 미리 나뉘어져 있어 계층적인 구조를 가지게 되므로 다른 구간의 사용자들이 정확한 위치를 제공하는 것과 특정 사용자들이 더 큰 구간의 정보를 제공하는 것으로부터 그 특정 사용자들이 정확히 어느 구간에 있는지를 유추할 수가 있고 익명성이 지켜지지 않을 수 있다. 이러한 문제점을 보완하기 위해 그래프 이론을 이용하여 동적으로 클러킹 구조를 형성하는 방법도 제안된바 있다[26].

5. 정 리

본고에서는 다양한 유비쿼터스 상황인지 커뮤니티 컴퓨팅에서 요구되는 정보보호 기법의 동향을 가장 주요한 측면 중 하나인 접근 제어 기술을 중심으로 정리하였다. 유비쿼터스 컴퓨팅의 특성상 고려할 필요성이 있는 상황 정보의 보호와 상황과 관련한 정책의 운용 등으로 확장되어 연구되고 있는 부분을 각각 포함하고 있다.

또한 이와 관련하여 상황 인지 컴퓨팅에서의 개인의 정보 유출에 대한 기술 동향을 다루었다. 상황 인지 컴퓨팅에서 개인 정보 보호를 위한 기법들 중 정보 누출, 클러킹(cloaking), 익명성 등에 대해 언급하였다.

본고의 범위에서 제외하였으나, 협업 개체 단위의 정보 접근 및 유출에 대한 제어나, RFID 관리를 포함한 인증 기법, 센서 네트워크의 정보보호 등 유비쿼터스 컴퓨팅의 다른 측면의 정보보호에 대해서도 많은 연구가 있어 왔다. 본고에서 정리된 내용들과 함께 상황인지 커뮤니티 컴퓨팅 시스템의 신뢰 구축에 적극적으로 적용된다면 보다 많은 분야에서 유비쿼터스 컴퓨팅이 유용하게 사용될 것으로 사료된다.

참고문헌

[1] 커뮤니티 컴퓨팅-위키백과, http://ko.wikipedia.org/wiki/커뮤니티_컴퓨팅

[2] L. Pareschi, D. Riboni, A. Agostini and C. Bettini, "Composition and Generalization of Context Data for Privacy Preservation", In Proc. of 6th IEEE International Conference on Pervasive Computing and Communications (PerCom), Mar, 2008, Hong Kong

[3] S. Jajodia, R. and S. Sandhu, "Toward a multilevel secure relational data model", In ACM SIGMOD Record, Vol. 20, No. 2, pp. 50-59, Jun., 1991

[4] E. Bertino and E. Ferrari, "Secure and selective dissemination of XML documents", In Transactions on Information and System Security (TISSEC), Vol. 5 No. 3, Aug., 2002

[5] P. Reddivari et al., "Policy based Access Control for a RDF Store", In Proc. of the Policy Management for the Web Workshop, May, 2005

[6] A. Jain and C. Farkas, "Secure resource description framework: an access control model", In Proc. of ACM symposium on Access control models and technologies(SACMAT '06), pp 121-129, 2006, Lake Tahoe, California, USA

[7] http://www.w3.org/TR/rdf-mt/#RDFSRules

[8] L. Qin and V. Atluri, "Concept-level access control for the Semantic Web", In Proc. of ACM workshop on XMLsecurity (XMLSEC '03), 2003

[9] U. Hengartner and P. Steenkiste, "Access Control to Information in Pervasive Computing Environments", In Proc. of HotOS, 2003

[10] L. Kagal, T. Finin and A. Joshi, "A policy language for a pervasive computing environment", In Proc. of IEEE 4th International Workshop on Policies for Distributed Systems and Networks, 2003

[11] H. Chen, F. Perich, T. Finin and A. Joshi, "SOUPA: standard ontology for ubiquitous and pervasive applications", In Proc. of Mobile and Ubiquitous Systems: Networking and Services (MOBIQUITOUS), Aug., 2004

[12] D. Kulkarni and A. Tripath, "Context-Aware Role-based Access Control in Pervasive Computing Systems", SACMAT '08, June 11-13, 2008, Colorado, USA

[13] P. Nasirifard, "Context-Aware Access Control for Collaborative Working Environments Based on Semantic Social Networks", In Proc. of International and Interdisciplinary Conference on Modeling and Using Context (CONTEXT'07), Roskilde, Denmark, 2007

[14] A. Samuel, A. Ghafoor and E. Bertino, "Context-Aware Adaptation of Access-Control Policies", IEEE Internet Computing, Vol. 12, No. 1, 2008

[15] A. Toninelli, R. Montanari, L. Kagal and O. Lassila, "A Semantic Context-Aware Access Control Framework for Secure Collaborations in Pervasive Computing Environments", In Proc. of International Semantic

Web Conference, 2006

[16] U. Hengartner and G. Zhong, "Distributed, Uncertainty- Aware access Control for Pervasive Computing", In Proc. of IEEE PerComW | '07, 2007

[17] R.J. Hulsebosch et. al, "Context Sensitive Access Control", In Proc. of SACMAT '05, June, 2005, Stockholm, Sweden

[18] E. Snekkenes, "Concepts for personal location privacy policies", In Proc. of the 3rd ACM conference on Electronic Commerce, pp. 48-57, 2001

[19] GeoPriv Location/Privacy (geopriv), http://www.ietf.org/html.charters/geopriv-charter.html

[20] L. Cranor, M. Langheinrich and M. Marchiori, "A P3P preference exchange language 1.0 (APPEL1.0), April 2002", http://www.w3.org/TR/P3P-preferences

[21] E.-S. Cho, K.-W. Lee and M. Hong, "Abstraction for Privacy in Context-Aware Environments", MATA-05, 2005

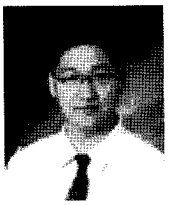
[22] F. L. Gandon and N. M. Sadeh, "A Semantic e-Wallet to Reconcile Privacy and Context Awareness." In Proc. of International Semantic Web Conference (ISWC2003), pp. 385-401, 2003, Sanivel Island, Florida, USA

[23] R. Wishart, K. Henricksen and J. Indulska, "Context obfuscation for privacy via ontological descriptions", In Proc. of Workshop on Location and Context-Awareness (LoCA), 2005

[24] L. Pareschi, D. Riboni and C. Bettini, "Protecting Users' Anonymity", In Proc. of Pervasive Computing Environments (PerCom), 2008

[25] Grusteser et. al, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking", In Proc. of Mobisys 2003

[26] B. Gedik and L. Liu, "A Customizable k-Anonymity Model for Protecting Location Privacy", In Proc. of IEEE ICDCS, 2005



김 윤 삼

2004 충북대학교 전기전자 및 컴퓨터공학부 컴퓨터전공 졸업(학사)
2006 충북대학교 전자계산학과 졸업(석사)
2005~2006 유비쿼터스 바이오정보기술 연구센터 연구원
2007~현재 충남대학교 컴퓨터공학과 박사과정
관심분야 : 개인정보보호, 상황인지 시스템, 시스템보안 등
E-mail : bijak@cnu.ac.kr

조 은 선

1991 서울대학교 계산통계학과 계산학전공 학사
1993 서울대학교 전산과학과 석사
1998 서울대학교 전산과학과 박사
1999~2000 한국과학기술원 연구원
2000~2001 아주대학교 정보통신전문대학원 조교수 대우
2002~2006 충북대학교 조교수
2006~현재 충남대학교 전기정보통신학부 컴퓨터전공 조교수
관심분야 : 정책 기술 언어, 상황인지 시스템, 상황데이터 모델링 및 언어 등
E-mail : eschough@cnu.ac.kr