개인정보보호 강화를 위한 동적 보안수준 결정

Dynamic Sensitivity Level Measurement for Privacy Protection

장인주(In Joo Jang)*, 유형선(Hyeong Seon Yoo)**

초 록

사회적요구와 기술 개발로 체계적인 개인정보관리와 보안 지침강화에도 불구하고, 개인정보 유출과 침해의 문제는 다양한 형태로 나타나고 있다. 이러한 개인정보를 관리함에 있어, 어떠한 정보를 보호할 것인가 하는 문제는 민감한 핵심 요소이다. 본 논문에서는 개인정보를 구성하는 각 속성정보의 관리 정책을 결정할 기준으로 속성정보의 동적 보안수준 측정법을 제시한다. 동적 보안수준 측정법은 개인정보의 가변적 특성을 측정 요소로 채택한다. 이 기법을 적용함으로, 개인의 각 속성정보 보안수준의 변화에 능동적으로 대처할 수 있는 정보관리 기능을 제공할 수 있다. 이는 기존 정보관리기법의 보안성을 더욱 높일 수 있으며, 통합 ID 관리 시스템이나 전자지갑과 같은 통합 시스템의 보안성 향상에 기여할 것으로 기대된다.

ABSTRACT

For social demand and technological development, systematic private information management and security guidance have been enhanced; however, the issue of leakage and invasion of private information is shown in many ways. In the management of such private information, the issue of how to protect such information is one of the sensitive key elements. As a criterion to decide the management policy of each property information consisting of private information, this article suggests Dynamic-Security-Level-Measurement for property information. DSLM adopts the variable characteristics of property information as the element of measurement. By applying this method, it is possible to provide information management functions to cope with the changes of each property information security level of an individual actively. It is expected that this will improve the security of previous information management methods even more and also contribute to the improvement of security in integrated systems such as the integrated ID management system and electronic wallet.

키워드 : 개인정보보호, 보안, 동적 보안수준 결정법
Information Technology, Security, Dynamic Security Level Measurement

---

본 논문은 인하대학교의 지원에 의하여 연구되었음.
* 주저자, 인하대학교 컴퓨터정보공학과 대우강사
** 교신저자, 인하대학교 컴퓨터정보공학과 교수
2012년 01월 30일 접수, 2012년 02월 11일 심사완료 후 2012년 02월 14일 게재확정.

1. 서 론

유비쿼터스 환경 및 전자정보 사회를 구축함에 있어 개인정보의 노출과 오남용의 위험은 치명적인 장애이며, 이 역기능을 막기 위한 많은 연구가 진행되고 있다[7, 10, 12, 21~23].

SSO(Single-Sign-On)기술이나 연합 ID관리(Federated ID Management) 기술들은 개인의 인터넷 서비스 사용증가와 함께 발생하는 사용자ID, 패스워드 증가와 같은 개인정보 관리부담의 문제를 해결하기위해 제안되었다[6, 13, 19]. 정책기반 접근통제(Policy-Based Access Control : PBAC) 기법이나 역할기반 접근통제(Role-Based Access Control : RBAC) 기법은 정보노출이 용이한 환경에서 정보에의 접근을 통제하기 위한 관리기법으로 제시되었다[15]. 정책협상기법(Policy Negotiation Scheme : PNS)이나 신뢰협상 기법(Trust Negotiation Scheme : TNS) 등은 서비스의 융합이나 연합의 과정에서 서로 다르게 설정된 정보관리 정책에 대해 합리적으로 반영하고 통제하기 위한 기술로 제안되었다[7, 8, 16, 20]. 그러나 이러한 기법들은 개인의 속성정보에 대해 정적특성으로 산출한 보안 수준에 맞추어 정책을 적용하였다. 이는 속성정보들의 변화된 보안수준을 고려하지 않은 정보관리기법으로 정보조합 등으로 생겨난 식별자등에 대처하지 못하는 취약점이 있다[19]. 개인정보란 그 특성상 개인이 생존해 있는 동안 행동하는 모든 과정에 사용되는 특정 개인에게 속한 정보이며, 한 번의 노출은 추후 어떠한 형태의 사후관리가 있더라도 그 정보의 주체인 개인에게는 치명적 이다. 따라서 노출 이전 발생할 수 있는 취약점에 대해 최대한의 보안성을 적용하여야 한다. 이에 본 논문에서는 동적으로 변화하는 개인정보의 보안수준을 반영하기 위해, 속성정보의 동적 보안 수준을 정의하고, 그 산출 방법을 제시하여 기존의 개인정보 관리기법의 보안성을 강화하고자 한다. 속성정보의 동적 보안 수준을 정의하기 위한 방법으로 형식 개념 분석 기법을 사용하였다.

2. 관련 연구

2.1 개인정보

개인정보(Personal Information)의 개념에 대해서는 다양한 견해가 존재하며 프라이버시(Privacy)와 개념상 동의로 쓰이기도 한다[2, 14, 19]. 개인정보란 개인을 특정 하는 사용자 개인의 실체에 관련된 모든 정보를 의미한다[1, 3, 4]. 이러한 개인정보는 개인의 실체를 특정 짓는 정도, 즉 식별의 정도에 따라 노출 시 발생하는 피해의 정도가 다르다[3, 15, 20, 21]. 따라서 본 논문에서는 개인정보를 신원을 확인할 수 있는 수준에 따라 개인 신원정보와 인증정보 그리고 일반정보와 부가정보로 분류하여 설명한다.

2.1.1 개인정보 분류

1) 개인 신원정보(Personal Identity Information) : 개인 신원정보란 사용자의 신원을 유일하게 식별할 수 있는 정보이다. 개인 신원정보는 주로 공공기관이 발급한다[4]. 따라서 개인 신원정보의 노출은 그 자체로 특정 개인을 지칭하는 것

으로 정보보호의 최상위 단계에서 관리되어야 한다. 한국의 주민등록번호와 미국의 SSN(Social Security Number) 등이 대표적이다. 이러한 정보는 거의 모든 분야에서 개인의 신원자료로 취급되어, 노출 될 경우 발생할 수 있는 침해가 가장 심각한 정보이다. 따라서 최상의 정보 보호기술을 적용해야 하는 매우 민감한 개인정보이다. 최근에는 지문과 홍채, DNA 등과 같은 신체 정보도 신원정보로 활용되고 있다.

2) 개인 인증정보(Personal Certification/Authentication Information) : 개인 인증정보란 SP가 권한 있는 사용자의 인증을 위해서 요구하는 정보를 의미한다. 서비스의 권한에 관한 확인 정보이므로, 노출 시에는 권한 없는 자가 불법적으로 개인의 권한을 남용하는 침해가 발생할 수 있다. 또한 해당 서비스 제공 영역에서는 특정 사용자를 식별하는 식별의 기능까지 지니고 있기에 제한적 영역 내에서의 신원정보라 할 수도 있다. 일반적으로 현재 대부분의 SP들은 ID와 비밀번호를 개인 인증정보로서 사용하고 있다. 그러나 확장되고 있는 인터넷 서비스 영역에 따라 한 개인이 이용하게 되는 서비스의 종류와 수가 급증하였으며, 이는 개인의 인증정보인 ID와 비밀번호의 양적 증가 또한 가져왔다. 때문에 정보보호기술 분야에서는 통합 인증 시스템에 대한 연구를 해왔다[2, 6, 11, 13, 19].

3) 개인 일반정보(Personal General Information) : 개인의 일반정보는 개인에 관련된 일반적인 정보이다. 대표적인 예는 사용자의 이름, 성별, 나이, 주소 등의 정보이며, 이 정보는 SP들이 사업전략 및 사업분석 등의 목적으로 수집하는 정보이다. 이러한 개인의 일반정보는 그 속성들의 결합을 통하여 식별 정보로 이용될 가능성이 있다. 따라서 속성정보의 변화된 보안수준이 판별되어야 하며, 그에 따른 정보처리 작업이 요구된다.

4) 개인 부가정보(Personal Optional Information) : 개인의 부가정보라 함은 SP의 서비스 영역에 따라 수집되는 개인에 관한 부가적 정보를 의미한다. 이러한 개인의 부가정보는 하나의 속성정보 단독으로 또는 다른 속성 정보와의 결합에 의하여도 식별기능을 지니지 않는다. 최근에는 사용자에게 개인화된 서비스(Personalized Service)를 제공하여 차별화된 서비스 환경을 구축하고, 경쟁력을 갖추기 위해 개인의 부가정보 수집에 더욱 적극적이며, 서비스영역을 넘어서 확장된 영역에 이르기까지 개인의 부가정보를 수집 한다.

본 논문에서는 개인정보보호를 위하여 개인의 신원정보와 인증정보 및 일반정보를 관리대상으로 한다. 부가정보의 경우 식별자의 차단으로 침해를 막을 수 있기에, 본 논문의 개인정보 관리대상에 포함시키지 않는다.

3. 개인정보의 동적 보안 수준

3.1 형식개념 분석기법의 적용

형식개념 분석 기법에서는 개념을 정의하

기 위해 객체집합, 속성집합, 관계집합의 세 가지 요소가 필요하다. 본 논문에서 다루는 개인정보관리 모델에 형식개념 분석기법을 적용하기 위해 다음과 같이 집합을 정의한다. 개인을 나타낼 수 있는 개인정보를 객체집합으로, 개인정보를 상세히 표현 할 수 있는 정보 값을 속성 집합으로. 그리고 객체 집합과 속성집합들의 이항관계를 나타내는 관계집합으로 정의하여 형식개념 분석기법에 적용한다. 개인정보 객체집합을 G, 개인정보 속성들의 집합을 N, 객체집합과 속성집합 사이의 이항관계를 R로 표현 할 때, 표현식 (1)과 같이 나타낼 수 있다[9, 24].

$$\begin{aligned} Context : D_G := \{G,\ N,\ R\} \\ \Rightarrow G := \{g_1,\ g_2,\ \cdots,\ g_n\} \\ \Rightarrow N := \{n_1,\ n_2,\ \cdots,\ n_n\} \\ \Rightarrow R \subseteq G \times N \end{aligned} \quad (1)$$

이때 하나의 객체 g1이 속성 n1을 가지고 있다면 이항관계 R의 정의에 따라 이항관계식은 표현 식 (2)로 표현 할 수 있다.

$$(g_1,\ n_1) \in R \Leftrightarrow \hat{r}(g_1,\ n_1) \quad (2)$$

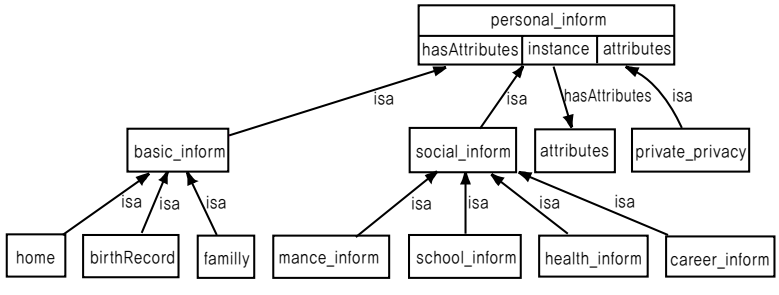
일차적으로 정의한 객체집합, 속성집합은 다음과 같다.

G : = {basic_inform, social_inform, private_privacy, identity}

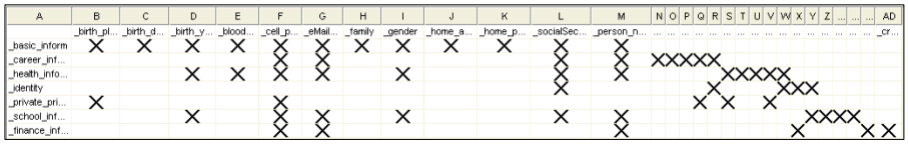
N : = {birth_year, birth_place, person_name, family, home_address, home_phone, SSN, ……}

정의된 개인정보의 객체 간 상-하위 관계는 온톨로지를 구성하여 <그림 1>과 같이 표현 할 수 있다[5].

<그림 1>을 통하여 개인정보 개념 집합의 구성원소인 각 객체간의 관계를 한 눈에 알 수 있으며, 이는 분석된 개인정보의 성질을



〈그림 1〉 개인정보 객체 간 상-하위 관계도



〈그림 2〉 개인정보의 객체-속성 간 이항관계도

쉽게 이해 할 수 있도록 한다. 또한 <그림 1>의 개인정보 객체집합의 원소에 대하여 (X, Y)의 쌍으로 표현하고, 서로에 대한 이항관계가 형성된 경우를 "X"로 표시하여 나타낸 결과 <그림 2>를 얻을 수 있다.

3.2 형식개념 분석 기법에 의해 표현된 개인 정보 속성

형식개념 분석 기법을 적용하여 관계집합으로 연결된 개인정보 속성을 표현하면 식 (3)과 같이 표현 할 수 있다.

$$X \mapsto X^R := \{n \in N | \hat{r}(g,\ n) \text{ for } g \in X\} \quad (3)$$
$$Y \mapsto Y^R := \{g \in G | \hat{r}(g,\ n) \text{ for } n \in Y\},$$
$$where\ X \subseteq G \wedge Y \subseteq N$$

식 (3)의 유도식으로 부터 식 (4)의 세 조건을 만족시킴을 알 수 있다.

$$(1)\ X_1 \subseteq X_2 \Rightarrow X_1^R \supseteq X_2^R, \quad (4)$$
$$(2)\ X \subseteq X^{RR},$$
$$(3)\ X^{RRR} = X^R$$

이때 형식 개념 $D_G := \{G,\ N,\ R\}$안에서 쌍을 이루는 (X, Y)가 $X \subseteq G \wedge Y \subseteq N$과 $X = Y^R \wedge Y = X^R$의 조건을 만족하면 X와 Y는 서로에게 형식 개념상에서 extent(범위)와 intent(의미)의 관계를 가지게 된다.

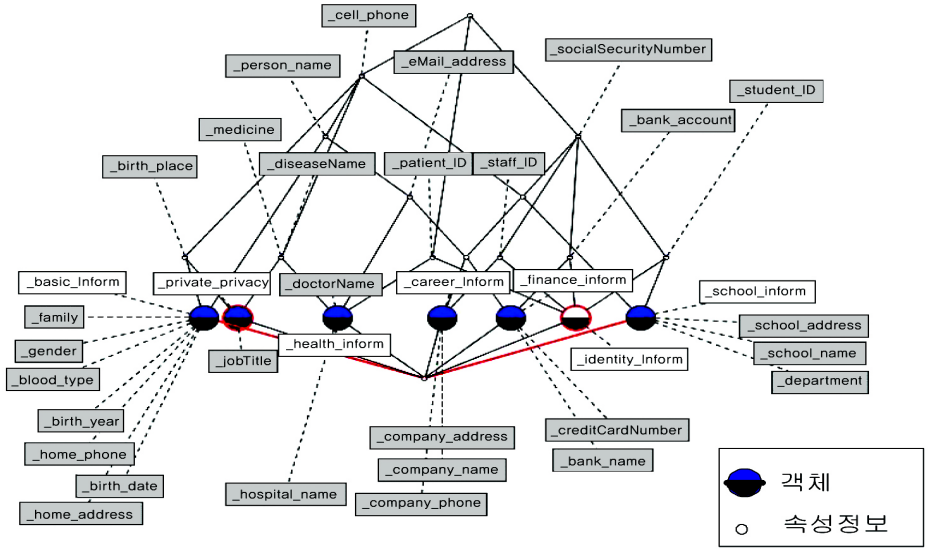
D_G의 $(X_1, Y_1) \leq (X_2, Y_2)$관계인 두 쌍 사이에 성립되는 관계 $X_1 \subseteq X_2 \Leftrightarrow Y_1 \supseteq Y_2$를 상-하위 개념의 관계라 한다. 모든 개인정보의 D_G 집합이 순차적 관계에 의하여 정의가 될 경우 개념 격자로 나타낼 수 있으며, 이 때 전체의 형식 개념에 대한 개념 격자를 $C(D_G)$로 표현한다. 하나의 객체 $g \in G$에 대하여 객체의 개념은 $\gamma g := (\{g\}^{RR},\ \{g\}^R)$로 나타낼 수 있으며, 전체 형식개념 $C(D_G)$안에서 객체의 최소화된 개념이 된다.

이러한 개념은 개념 격자를 이용하여 가시화 할 수 있다. Wille는 표현식 (5)와 같이 하한(infimum)과 상한(supremum)의 의미를 나타냈으며, 이를 개념 격자 표현에 도입하여 가시성을 높였다[1].

$$\text{하한;}\ \wedge_{t \in T}(X_t, Y_t) = \left(\cap_{t \in T} X_t, (\cup_{t \in T} Y_t)^{RR}\right) \quad (5)$$
$$\text{상한;}\ \vee_{t \in T}(X_t, Y_t) = \left((\cup_{t \in T} X_t)^{RR}, \cap_{t \in T} Y_t\right)$$

<그림 3>은 식 (5)의 하한점과 상한점을 반영하여 표시된 개인정보에 관한 개념 격자의 선형다이어그램이다.

<그림 3>은 개인정보를 활동영역에 따라 분류한 각 개념들이 지닌 속성 값과 쌍을 이루는 이항관계를 개념 격자로 구성하고 이를 가시화 시킨 다이어그램이다. 각각의 속성 값이 어떠한 개인정보 객체와 연계되어 있는지 한 눈에 알 수 있다. 사용한 도구는 FCAView 1.0이며, 이를 Protege 3.0에 연동하여 Lattice로 얻은 다이어그램이다[17]. 개념 격자로 형성된 속성들을 분석하여 새롭게 형성된 개념들을 확인하기 용이하며, 개념들의 위상변화를 파악하기 쉽다. 정보개념의 위상변화는 보안수준의 변화로 해석 될 수 있다. 즉, 형식개념 격자의 생성을 통해 속성정보의 보안수준의 변화를 쉽게 파악할 수 있다. 본 논문에서는 이를 수치화 하여 속성정보의 보안수준을 산출하는 동적 특성 값으로 사용하였다.



〈그림 3〉 개인정보의 객체와 속성간 개념의 선형 다이어그램

3.3 동적 보안수준 산출식

앞에서 언급했듯이 개인정보의 가장 큰 특징은 특정 개인에 관한 정보를 지니며, 각 속성정보의 특성에 따라 프라이버시보호에 대한 민감도에 끼치는 영향이 결정된다. 프라이버시보호 민감도에 영향을 미치는 특성요소는 다음과 같이 분류해 볼 수 있다.

식별성(Identity) : 특정 속성정보는 특정인을 식별하는 기능을 지닌다. 이는 노출될 경우 개인의 프라이버시 침해의 근간이 될 수 있으며, 그 피해의 영역이 매우 크다.

사용자 민감도(User-Privacy) : 개인정보는 정보의 주체인 개인의 주관적인 견해가 있다. 즉 사용자 개인별로 각각의 속성정보에 따라 정보공개로 인해 느껴지는 불편과 침해의 정도가 다르다. 이는 많은 연구자들도 지적하였으며[6, 10] 이를 사용자 개인의 프라이버시 정책이라 명명하고 개인정보 관리에 반영한다.

속성정보의 함축도(Connotation degree) : 특정 개인정보의 속성은 하나의 속성 안에 몇 개의 의미를 함축하고 있는 경우를 발견하게 된다. 예를 들어 대한민국의 경우 주민등록 번호에는 개인에 관한 많은 의미가 포함 되어있다. 개인의 신원 정보로서의 생년월일뿐만 아니라, 태어난 지역과 성별까지 알 수 있는 다수의 의미를 담고 있는 하나의 속성이다.

따라서 개인정보속성의 보안상 민감도(Sensitivity Level)를 측정하기 위해서는 위의 특성요소가 모두 반영되어야 한다. 또한, 보안상 민감도는 해당 속성정보의 보안정책에 반영되어야 하는 성질이며, 이 민감도가 높을수록 보안정책의 강도 또한 높아져야 한다. 즉 보안상 민감도는 해당 속성정보의 보안수준을 나타낸다고 할 수 있으며, 이하 보안수준이라 명한다. 속성정보의 보안상 민감도를 산

출하는 적합한 식을 수립하기 위하여 각 특성요소를 반영하는 유사개념의 수학적 모델링인 여측 수익 산출식을 적용하였다. 이와 같은 적용을 통하여 보안 수준 산출식을 식 (6)과 같이 수립하였다.

$$Sensitivity\,Level: \quad (6)$$
$$S_L(a) := \alpha \cdot I(a) + \beta \cdot P(a) + \gamma \cdot C(a)$$
$$I(a) = \begin{cases} 1, & where\ a \in Identity \\ 0, & where\ a \notin Identity \end{cases}$$
$$P(a) = \begin{cases} 1, & where\ a \in user-privacy \\ 0, & where\ a \notin user-privacy \end{cases}$$
$$C(a) = \begin{cases} 1, & where\ a \in connotation-value \\ 0, & where\ a \notin connotation-value \end{cases}$$

식 (6)에서 α, β그리고 γ는 각 특성요소가 지니는 무게지수이다. 보안수준 산출식에서의 무게지수는 각 속성의 특성이 민감도에 미치는 영향력을 반영하는 값이다. 즉 각 특성요소가 속성정보의 보안수준을 결정하는 과정에 미치는 영향은 환경에 따라 조금씩 다를 것으로 예측되며, 이를 무게지수로 나타낼 수 있다. 그러나 본 논문에서는 무게지수의 적합한 값에 대한 연구를 포함하지 않았으며, 동일한 영향을 미친다는 가정 하에 1로 적용하여 산출식을 수립하였다.

이로써, 보안수준 산출식 (6)을 이용하여 속성정보의 보안수준 S_L을 산출하여 속성정보의 보안수준을 평가하고, 이에 적합한 정책 적용을 할 수 있다. 그러나, SP의 요구에 따라 이루어지는 정보의 공개는 각 속성정보의 보안수준을 변화 시킬 수 있음이 나타난다. 즉 식별력이 없는 공개 정보들이 서로 연관성을 나타내며 식별자 역할을 할 수 있음이 발견된다[18, 20]. 이러한 현상을 식별자의 재생산 기능이라 명하며, 이러한 현상을 보안수준 결정에 반영하기 위해 본 논문에서는 형식 개념 분석 기법을 이용하였다. 정보의 속성과 정보를 제공받은 객체간의 개념 격자를 수립하고, 이를 분석함으로 변화되는 보안수준을 측정한다. 활동영역이 많은 속성정보는 노출될 경우, 다른 정보들과 연계하여 보안상 민감한 인증정보나 신원정보로의 역할을 수행할 수 있다는 특성을 반영한 것으로, 이를 동적보안 수준이라 명한다.

3.4 속성정보의 동적 보안수준

<그림 1>과 같이 표현된 개인정보는 객체 집합 G와 속성들의 집합 N 및 두 집합간의 이항관계로 표현된다. 이때 각각의 속성과 객체 개념과의 관계는 유도식 (7)과 같이 표현된다.

$$\begin{cases} D_G := \{G, N, R\} \\ G := \{g_1, g_2, \cdots, g_n\} \\ N := \{n_1, n_2, \cdots, n_n\} \end{cases} \quad (7)$$
$$\Rightarrow \begin{cases} \hat{r}(g_1, n_k),\ N_1 := \{n_{11}, n_{12}, \cdots, n_{1k}\} \\ \qquad\qquad \vdots \\ \hat{r}(g_n, n_k),\ N_n := \{n_{n1}, n_{n2}, \cdots, n_{nk}\} \end{cases}$$
$$; where\ N_i \subseteq N \wedge k := order\,of\ N_i$$

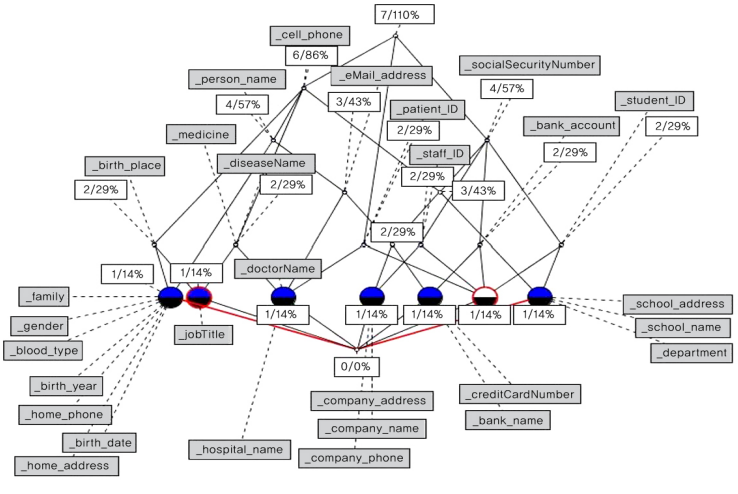
어떤 개인정보의 속성 n이 객체의 개념 g_i와 g_j에 공개된 속성정보인 경우, 그 의미는 $\exists n := (n \in N_i) \wedge (n \in N_j)$와 같이 나타낼 수 있다. 이때 속성 n을 포함하는 모든 속성집합에 대해 표현하면, $n \in N_{ij}$, $N_{ij} := N_i \cap N_j$로 나타낼 수 있으며, 이는 개인정보의 속성 n이 속성 집합 N_i와 N_j의 원소임을 의미한

다. 이러한 표현 방법에 의하여 개인정보 속성 n의 결합도는 식 (8)과 같이 표현된다. 속성 n의 결합도란 속성 n이 몇 개의 객체 개념에 연결되어 있는가를 측정하는 것이며, 이는 속성정보 n의 정보 공개 및 정보 값의 노출 정도를 의미한다.

$$D_C(n) = count(i), \quad (8)$$
$$where\ (n \in N_i),\ i = 1,\ 2,\ \cdots,\ n.$$
$$where\ \ \exists n = \{n \in N\},$$
$$N_{1,2,\cdots,n} := N_1 \cap N_2 \cap \cdots \cap N_n$$

$D_c(a)$라 표현된 경우는 개인정보속성 a의 결합도를 의미하는 것이다. 이때 결합되어 있는 속성집합의 개수를 의미하는 $count(i)$값이 개인정보속성 a의 결합도를 의미하며, 본 논문에서는 사용자가 등록한 전체의 객체 개념에 백분율로 나타낸다. 백분율로 환산된 개인정보속성 a의 결합도는 해당 속성정보의 동적 특성으로 정의된다. 이 동적특성은 개인정보 속성의 민감도 산출식 즉 보안수준 산출식에 이용되어 개인정보 속성의 최종 보안수준을 결정하게 된다. 즉 최종적인 개인정보 속성의 보안수준은 식 (8)에서 얻은 값이 반영된 식 (9)와 같이 산출된다. 제 3.2절에서 형식개념분석 기법을 적용시킨 개인정보에 대한 결합도는 개념 격자에 계산식을 적용하여 <그림 4>와 같이 얻을 수 있으며, 이는 각 속성의 결합도를 한 눈에 보여준다.

$$Sensitivity\ Level: \quad (9)$$
$$S_L(a) := \alpha \cdot I(a) + \beta \cdot P(a) + \gamma \cdot C(a) + \delta \cdot D_c(a)$$
$$I(a) = \begin{cases} 1, where\ a \in Identity \\ 0, where\ a \notin Identity \end{cases}$$
$$P(a) = \begin{cases} 1, where\ a \in user-privacy \\ 0, where\ a \notin user-privacy \end{cases}$$
$$C(a) = \begin{cases} 1, where\ a \in connotation-value \\ 0, where\ a \notin connotation-value \end{cases}$$
$$D_c(a) = count(i)$$
$$where\ n \in N_i, i = 1,\ 2,\ \cdots,\ n$$



〈그림 4〉 객체와 속성 간 선형 다이어그램

각 속성정보의 개념 노드마다 지니는 결합도를 백분율로 표현한 것이다. <그림 4>에서 보듯이 _cell_phone의 결합도는 86% 이며, 가장 민감한 신원정보로 분류되는 _socialSecurity Number의 결합도는 57%이다. 결합도만으로 분석을 할 경우 _cell_phone의 정보가 노출될 경우 더 높은 침해의 경로를 제공하게 된다.

즉_cell_phone과 함께 노출된 정보를 수집하여 _cell_phone을 중심으로 재조합하면 정보의 주체인 개인을 식별할 가능성이 가장 높으며, 많은 정보를 수집할 수 있다는 결론이다. 이와 같이 결합도는 개인의 정보이용 성향과 정보에 따라 동적인 값을 지니게 된다. 이는 개인정보의 보안 수준이 동적인 성질을 지니게 되며, 이를 반영한 보안정책의 적용이 이루어 질 때, 보안성 높은 개인정보 관리를 할 수 있게 된다.

4. 동적 보안수준 산출과 의미분석

본 절에서는 실제 온라인 서비스에 가입할 경우, 제공을 요구받는 기본적인 개인정보 속성을 반영하여 동적 보안 수준을 산출하고, 그 값이 지니는 의미를 고찰해 본다.

〈그림 5〉 서비스의 정보제공 요청화면

가상의 홍길동이라는 인물이 쇼핑몰(eShop)과 대학병원(eHospital), 은행(eBank)에 <그림 5>와 같이 회원가입을 하게 될 경우 제공하는 기본적인 필수 정보를 대상으로 형식개념분석 기법을 적용하여 각 속성의 보안수준 즉 민감도를 측정하였다.

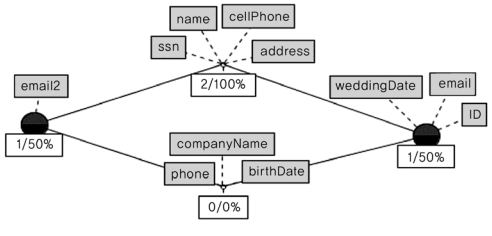
4.1 동적 보안수준 산출(예1)

가상의 인물 홍길동이 쇼핑몰과 병원서비스를 이용하기 위하여 온라인상으로 회원가입을 한 후, 두 SP에게 공개한 정보의 속성에 대하여 형식개념 격자를 구성하면, <그림 6>의 결과를 얻을 수 있다.

	ID	address	birthDate	cellPhone	compan...	email	email2	name	phone	ssn	wedding..
eShop	X	X		X		X		X		X	X
eHospital		X		X			X	X		X	

〈그림 6〉 예 1 정보객체와 속성 간 이항관계

<그림 7>에 대한 선형 다이어그램은 <그림 8>와 같이 얻을 수 있으며, 각 속성들의 결합도를 나타낼 수 있다.



〈그림 7〉 예 1 개념의 선형 다이어그램

이 경우 선형 다이어그램만을 본다면 속성 cellPhone은 ssn과 같은 보안수준으로 관리되어야 함을 예측 할 수 있다.

〈표 1〉 예 1의 개인정보 각 속성의 특성값과 보안수준 산출값

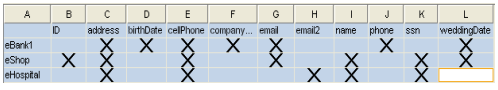
예 1 (쇼핑몰 · 병원)	$I(a)$	$P(a)$	$C(a)$	$D_c(a)$	$S_L := \alpha \cdot I(a) + \beta \cdot P(a) + \gamma \cdot C(a) + \beta \cdot D_c(a)$
name				1	1
ID	1			0.5	1.5
ssn	1		1	1	3
address				1	1
birthDate				0	0
cellPhone	1			1	2
company_Name				0	0
email	1			0.5	1.5
email2	1			0.5	1.5
phone				0	0
wedding_Date				0.5	0.5

<표 1>에서 보듯이 예시 1의 경우 속성 ssn의 그러나 개인정보의 보안수준 산출을 위해서는 식 (9)와 같이 정보속성의 특성값이 함께 반영되어야 한다. 다만, 본 논문에서는 $P(a)$의 값, 즉 사용자 개인의 프라이버시 정책은 지극히 개인의 주관적 의사이기에 반영하지 않았으며, 각 특성요소의 무게지수 값은 동일하게 1로 반영을 하여 계산하였다.

보안수준 산출값은 3, 속성 cellPhone의 보안수준 산출값은 2로 결정이 된다. 보안수준 산출값이 말해주듯, ssn은 최상의 보안수준으로 정보관리가 이루어져야 함을 명확히 나타낸다. 이와 같이 형식개념 분석의 결과로 얻은 <표 1>은 적용되고 있는 정보관리 정책이 각 속성정보에 대하여 적합한 보안수준을 유지하고 있는가를 판단하는 근거의 역할을 한다.

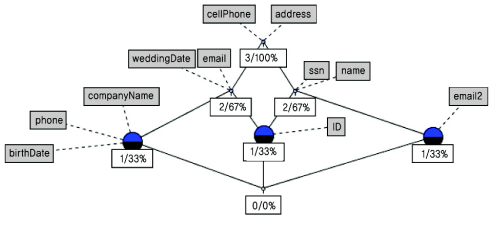
4.2 동적 보안수준 산출(예 2)

예 2에서는 가상의 인물 홍길동이 쇼핑몰과 병원 서비스의 회원가입 후 은행 서비스를 이용하기 위하여 자신의 정보를 SP에게 공개 한 후, <그림 8>와 같은 결과를 얻었다.



〈그림 8〉 예 2의 객체와 속성 간 이항관계

<그림 8>의 형식개념 격자로부터 얻어지는 선형 다이어그램은 <그림 9>와 같다.



〈그림 9〉 예 2 개념의 선형다이어그램

이때 각 속성정보들의 결합도 $D_c(a)$의 값이 변화한 것을 알 수 있다. 변화한 결합도를 보안수준 산출식 (9)에 적용하여 각 속성정보의 보안수준을 산출하면 <표 2>와 같은 결과를 얻을 수 있다. 산출과정은 예시 1의 경우와 동일한 방법을 적용하였다. <표 2>의 결과를 <표 1>의 결과와 비교하면, 각 속성정보들에 대하여 보안수준이 변화되었음을 알 수 있다. 예시 1의 경우에서와 같이 속성 ssn의 보안수준은 속성 cellPhone의 보안수준보다 높게 산출이 되었으나, 속성정보 email과 email2의 보안수준에는 변화가 생겼음을 보여준다. 속성 email의 보안수준이 email2의 보안수준 보다 높게 변화되었으며 이는 email의 공개가 요구될 때 email2의 경우보다 더욱 신중해야 함을 의미한다. 즉 정보수집자가 수

집된 홍길동의 정보로 프로파일을 생성할 때 홍길동의 식별자 역할에 있어 속성정보 email의 경우가 email2의 경우보다 더욱 강한 식별력을 지닐 수 있으며, email의 속성값으로 홍길동의 더 많은 정보를 수집할 수 있음을 의미한다. 따라서 정보관리에 있어, 보안 정책 적용시 변화된 보안수준이 반영되어야 보다 안전한 정보관리를 기대 할 수 있다.

〈표 2〉 예 2의 개인정보 각 속성의 특성값과 보안수준 산출값

예 1 (쇼핑몰·병원)	$I(a)$	$P(a)$	$C(a)$	$D_c(a)$	$S_L := \alpha \cdot I(a) + \beta \cdot P(a) + \gamma \cdot C(a) + \beta \cdot D_c(a)$
name				0.67	0.67
ID	1			0.33	1.33
ssn	1		1	0.67	2.67
address				1	1
birthDate				0.33	0.33
cellPhone	1			1	2
com-pany_Name				0.33	0.33
email	1			0.67	1.67
email2	1			0.33	1.33
phone				0.33	0.33
wed-ding_Date				0.67	0.67

5. 결 론

다양한 온라인 서비스의 제공과 사용으로 다루어지는 개인의 속성정보의 양과 종류도 빠르게 늘어나고 세분화 되었다. 이러한 사용환경 아래서 많은 암호기술과 인증기술이 정보보호의 기능을 강화하고 있으나, 관련 기술의 발달은 개인정보의 수집력 또한 증가시켜 왔다. 개인정보란 개인이 생존기간 동안 사용하게 되는 정보이기에, 한 번의 노출이 정보주체자인 개인에게 미치는 침해의 정도는 정확한 예측이 불가능하며, 그 후유증은 매우 크다. 본 논문의 예시 1과 예시 2에서 보았듯, 개인의 속성정보는 가변적인 보안수준을 지닌다. 기존의 정보관리 기법으로는 수집된 정보에서 재생산되는 식별자로 발생하는 침해에 취약할 수밖에 없다. 이는 현재의 정보관리 정책이 변화한 속성정보에 대하여 변화된 보안 정책을 반영하지 못하기 때문이다. 본 논문에서 제시한 동적보안 수준 산출식은 이러한 속성정보 보안수준 변화를 수치화하여 제공하기에 정책적용에 명확한 기준으로 사용이 가능하다. 단 각 특성요소 간 보안 수준에 미치는 영향력을 산출하여 무게 지수를 산정하는 과제는 추후 계속되는 연구결과로 발표하고자 한다.

참 고 문 헌

[1] 남기효, 박상중, 강형석, 남기환, 김성인, “개인정보보호 기술의 최신 동향과 향후 전망”, 정보보호학회논문지, 제18권, 제6호, pp. 11-19, 2009.

[2] 윤상오, “전자정부 구현을 위한 개인 정보보호 정책에 관한 연구 : 정부신뢰 구축의 관점에서”, 한국지역정보화학회지, 제12권, 제2호, pp. 1-29, 2009.

[3] 이재광, 장종수, 박기식, “사이버 공간에서의 개인정보보호”, 한국정보사회학회, 정보와 사회, 제12권, pp. 51-65, 2007.

[4] 이해규, “인터넷 환경에서의 사용자 중심 ID 정보관리 모델에 관한 연구”, 정보보호학회논문지, 제19권, 제3호, pp. 37-50, 2009.

[5] 장인주, “User-centric Personal Information Management Model for Privacy Protection,” 인하대학교, Thesis, 2010.

[6] Ahn, G. J., “User-centric Privacy Management for Federated Identity Management,” Collaborate Com ’07, pp. 187-195, 2007.

[7] Bhargav-Spantzel, Squicciarini, A. C., and Bertino, E., “Integrating Federated Digital Identity Management and trust Negotiation-issues and solutions,” Security and Privacy Magazine, IEEE, Vol. 5, No. 2, pp. 55-64, 2007.

[8] Bonatti, P., “Driving and Monitoring Provisional Trust Negotiation with Meta-policies,” IEEE POLICY ’05, pp. 14-23, 2005.

[9] Burmeister, P., “Treating Incomplete Knowledge in Formal Concept Analysis,” LNAI 3626, pp. 114-126, 2005.

[10] Canard, S., “Identity Federation and Privacy : One Step Beyond,” DIM ’08, pp. 25-37, 2008.

[11] Deng, M., Cock, D. D., and Preneel, B., “toward a cross-context identity management framework in e-health,” Online Information Review, Vol. 33, No. 3, pp. 422-442, 2009.

[12] Garcon, K., “Security and Privacy System Architecture for an e-Hospital Environment,” in Idtrust ’08 IBE, PBE, automated encryption processing, 2008.

[13] Josang, A., AlZomai, M., and Suriadi, S. “Usability and Privacy in Identity Management Architectures,” AISW ’07, pp. 143-152, 2007.

[14] Josang, A., Fabre, J., Hay, B., Dalziel, J., and Pope, S., “Trust Requirements in Identity Management,” Proceeding of the AISW ’05, pp. 99-108, 2005.

[15] Park, H.-A., “Privacy-Aware Access Control through Negotiation in Daily Life Service,” LNCS 5075, pp. 514-519, 2008.

[16] Preibusch, S., “Ubiquitous social networks-opportunities and challenges for privacy-aware user modelling,” DM. UM ’07, pp. 698-721, 2007.

[17] Protege 3.1. [cited; Available from : http ://protege.stanford.edu/doc/users.html.

[18] Qian Wang, Wiangling Shi, “Privacy Protection Based on l-Diversity,” WCSE ’09, pp. 367-372, 2009.

[19] Satchell, C., Shanks, G., Howard, S., and Murphy, J., “Identity crisis : user perspectives on multiplicity and control in federated identity management,” Behaviour and Information Technology ’09, pp. 1-12, 2009.

[20] Spantzel, A. B., Squiiciiarini, A. C., and Bertino, E., “Trust Negotiations in Identity Management,” IEEE S&P 2007, pp. 55-63, 2007.

[21] Squicciarini, A. C., Elisa Bertino, E. Ferrari, and I. Ray, “Achieving Privacy in Trust Negotiations with an Ontology-Based Approach,” IEEE Transactions on

Dependable and Secure Computing, Vol. 3, pp. 13-31, 2004.

[22] Squicciarini, A. C. and Barghav, A., "Trust Negotiations with Customizable Anonymity," Proceed of the IEEE/WIC/ACM, pp. 69-72, 2006.

[23] Sweeney, L., "k-Anonymity : A Model for protecting Privacy Fuzziness and Knowledge-based Systems," Vol. 10, No. 5, pp. 557-570, 2002.

[24] Wille, R., "Formal Concept Analysis as Mathematical Theory of Concepts and Concept Hierarchies," LNAI 3626, pp. 1-33, 2005.

저 자 소 개

장인주 (E-mail : jangij@dreamwiz.com)
1991년 인하대학교 자동화공학과 (학사)
2005년 인하대학교 컴퓨터정보공학과 (석사)
2010년 인하대학교 컴퓨터정보공학과 (박사)
2011년~현재 인하대학교 컴퓨터정보공학과 대우강사
관심분야 Applied Cryptography, Scientific Computation

유형선 (E-mail : hsyoo@inha.ac.kr)
1974년 인하대학교 기계공학과 (학사)
1976년 한국과학기술원 기계공학과 (석사)
1983년 Ghent University, Belgium 기계공학 (박사)
1979년~현재 인하대학교 컴퓨터정보공학과 교수
관심분야 Applied Cryptography, Scientific Computation