개인정보 노출을 예방하는 방법에 관한 연구

이기성* · 안효범** · 이수연***

요 약

정보통신망의 발전과 함께 인터넷 사용 인구와 다양한 개방적 구조의 서비스 이용률이 지속적으로 증가하고 있다. 하지만 서비스 이용자들의 보안의식은 크게 달라지지 않아 서비스 이용자들의 직접적인 입력으로 인터넷상에 노출되는 개인정보가 늘어나고 있는 실정이며 이로 인한 이차적인 침해로 인하여 개인에게 정신적인 피해와 금전적 손괴 심지어는 신체적인 위험을 주는 각종 범죄가 행해지고 있다. 서비스 이용자의 직접적인 입력으로 인한 개인정보 노출을 예방하기 위해서는 게시물을 등록하는 서비스 이용자에게 게시물에 포함된 개인정보와 개인정보 노출의 위험성을 인지시켜 이차적 침해의 위험성이 높은 개인정보는 게시하지 않도록 해야 한다. 본 논문에서는 게시물의 노출 수준과 개인정보자산 가치를 이용하여 각 개인정보의 위험수준을 산정하는 모델과 게시판과 같은 서비스에서 개인정보노출정도에 따른 위험도를 사용하는 방법을 보였다.

A Study on a Prevention Method for Personal Information Exposure

Ki-Sung Lee* · Hyo-Beom Ahn** · Su-Youn Lee***

ABSTRACT

Along with the development of Internet services such as Social Network Service (SNS) and blog Service, the privacy is very important in these services. But personal data is not safety from exposure to internet service. If personal data is leak out, the privacy is disclosed to hacker or illegal person and the personal information can be used in a cyber crime as phishing attacks. Therefore, the model and method that protects to disclose privacy is requested in SNS and blog services. The model must evaluate degree of exposure to protect privacy and the method protects personal information from Internet services. This paper proposes a model to evaluate risk for privacy with property of personal data and exposure level of internet service such as bulletin board. Also, we show a method using degree of risk to evaluate with a proposed model at bulletin board.

Key words : Personal Information Exposure, Information Exposure Prevention

접수일(2012년 2월 28일), 수정일(1차: 2012년 3월 14일), 게재확정일(2012년 3월 19일)

* 공주대학교 정보통신공학부
** 공주대학교 정보통신공학부 (교신저자)
*** 백석문화대학교 인터넷정보학부

1. 서 론

정보통신망의 지속적인 발전과 스마트 모바일 기기의 보급으로 개인의 인터넷 이용률이 지속적으로 증가하고 있다[1]. 더불어 인터넷을 통한 비즈니스의 일환으로 다양한 콘텐츠를 제공하는 사이트들이 급속히 증가하고 있으며 이와 같은 대부분의 사이트들은 서비스 이용자들의 이용 편의와 참여를 위하여 게시판과 같은 게시물 등록 기능을 제공하고 있다. 특히 최근에는 블로그, 소셜 네트워크, 콘텐츠 커뮤니티 등 국내외의 소셜 미디어 서비스 이용자와 게시물이 폭발적으로 증가하고 있는 추세이다.

하지만 인터넷 이용률의 지속적인 증가에 비해 서비스 이용자들의 보안 의식수준은 제자리걸음을 하고 있으며 이에 따른 역기능 또한 증가하고 있는 실정이다[2]. 보안 의식이 부족한 연령층의 서비스 이용자들이 점점 늘어남에 따라 서비스 이용자들의 직접적인 입력으로 인터넷상에 노출 되어지는 개인정보가 늘어나고 있으며 이로 인하여 노출된 개인정보를 이용한 명의도용 및 계정탈취, 피싱, 스팸 메시지, 프라이버시 침해, 유괴 등 개인에게 정신적인 피해와 금전적 손괴 심지어는 신체적인 위험을 주는 각종 범죄가 행해지고 있다[3,4].

소셜 미디어 등의 개방적 구조의 서비스 이용자들에 의한 직접적인 입력으로 발생하는 개인정보의 노출과 이에 따라 발생하는 이차적인 침해 사고의 피해를 예방하기 위해서는 일차적으로 개인정보보호 의식이 부족한 서비스 이용자들에게 게시물에 포함된 개인정보와 개인정보 노출 시의 위험성을 인식하도록 해야 한다. 따라서 본 논문에서는 서비스 이용자의 직접적인 입력으로 개인정보가 노출될 경우의 위험수준을 산정하는 모델을 제시하고 해당 모델을 게시물 등록과정에 적용함으로서 서비스 이용자가 효과적으로 개인정보 노출의 위험성에 대하여 인식하도록 하는 방법을 제안한다.

본 논문의 2장에서는 개인정보 노출차단과 개인정보 노출의 위험도 계량화에 관련한 연구를 살펴보며, 3장은 개인정보가 노출될 경우의 위험수준을 산정하는 모델을 제시하며, 4장에서는 3장에서 제시한 모델을 적용하여 개선된 게시물 등록과정을 제안하고, 5장에서는 결론을 설명한다.

2. 관련 연구

2.1 개인정보의 노출차단

개인정보 노출차단은 서비스 이용자나 서비스 제공자가 서비스나 콘텐츠를 제공할 때, 실수로 자신이나 특정인의 개인정보를 노출함으로써 발생하는 사고를 방지하기 위해 서비스나 콘텐츠 제공 직전에 개인정보 노출에 대해 자동으로 사전 점검을 수행하여 부주의한 개인정보 노출을 차단하는 기술이다[5].

행정안전부는 '공공기관 홈페이지 개인정보 노출방지 가이드라인'에서 콘텐츠 생성단계에서 개인정보노출을 방지하기 위해 홈페이지 이용자가 게시물을 게재하거나 열람하는 시점에서 개인정보 포함여부를 점검하여 노출을 차단하는 개인정보 필터링 시스템 적용을 권고하였으며 이에 따라 정보보호 기업들은 개인정보의 필터링 시스템을 개발하여 출시하였다[6].

하지만 주로 업무 담당자가 콘텐츠를 생성하는 공공기관을 주요 대상으로 출시한 해당 개인정보 필터링 시스템은 개방적 구조의 서비스를 운영하는 민간기업에 적용하는데 어려움이 있다. 기존의 개인정보 필터링 시스템은 관리자의 정책에 의하여 일방적으로 개인정보의 노출을 차단함으로서 개인정보 노출을 예방하는 방식이지만 주로 서비스 이용자가 개인적인 내용의 콘텐츠를 생성하는 개방적 구조의 서비스 환경에서는 <표 1>의 내용과 같이 일방적 구조의 서비스에 비하여 서비스 이용자가 소량의 개인정보를 여러 게시물에서 자주 다루기 때문에 기존의 개인정보 필터링 시스템을 적용한다면 서비스 이용에 큰 불편을 초래할 것이다.

<표 1> 개방성에 따른 게시물의 특성 비교

특성 비교	일방적 구조	개방적 구조
콘텐츠 생성 주체	업무 담당자	서비스 이용자
게시물의 성격	공공적	개인적
게시물의 수	비교적 소수	비교적 다수
게시물의 게시빈도	비교적 드물게	비교적 빈번
개인정보 노출량	대량	소량

이러한 이유로 개방적 구조의 서비스를 운영하는 민간기업에서는 개인정보 필터링 시스템을 도입하지 않고 있는 실정이며 따라서 날로 성장해가는 개방적 구조의 서비스 환경에서 서비스 이용자의 직접적인 입력으로 인한 개인정보노출이 심각해질 것으로 예상된다. 이러한 개방적 구조의 서비스 환경에서의 개인정보 노출을 예방하기 위해서는 콘텐츠를 생성하는 서비스 이용자가 게시물에 포함된 개인정보와 개인정보의 노출 시 위험성을 인지하고 이차적 침해의 위험성이 높은 개인정보는 게시하지 않도록 유도하는 방안이 필요하다.

2.2 개인정보 노출의 위험도 계량화

개인정보 유·노출 시의 위험수준을 평가하는 방법으로 개인정보 영향평가의 개인정보 위험도 산정이 있다. 개인정보 영향평가는 개인정보를 활용하는 새로운 정보시스템의 도입이나 개인정보 취급이 수반되는 기존 정보 시스템의 중대한 변경 시 동 시스템의 구축·운영·변경 등이 프라이버시에 미치는 영향에 대하여 사전에 조사·예측·검토하여 개선방안을 도출하는 체계적인 절차를 말하며 개인정보 영향평가의 위험도 산정은 개인정보가 포함된 업무를 자산으로 보고 업무 내 개인정보의 조합수준에 따라 자산가치를 선정하여 자산가치, 발생가능성, 법적준거성을 조합하여 위험도를 평가하여 합산하는 방법이다[7].

개인정보 영향평가의 위험도 산정방법은 공공기관을 주요대상으로 하고 있으며 기관이나 기업의 입장에서 다양한 측면의 위험을 고려하여 위험도를 산정한다. 하지만 개방적 구조의 서비스 환경에서는 콘텐츠 생성의 주체가 서비스 이용자이기 때문에 기관이나 기업의 입장에서 발생가능성, 법적준거성 등의 다양한 측면의 위험요인을 고려하는 위험도 산정 모델이 아닌 서비스 이용자의 입장에서 각 개인정보가 노출될 경우만의 위험정도를 고려하여 위험도를 산정하는 모델이 요구된다.

3. 노출 시 위험수준 산정 모델

본 논문에서 제안하는 위험수준 산정 모델에서는 우선 각 개인정보의 자산가치와 서비스 이용자의 입력으로 인하여 개인정보가 노출 되었을 경우 해당하는 서비스에서 노출되는 수준과의 관계를 고려해보면 다음과 같이 정리 할 수 있다.

- 자산가치의 값이 클수록 외부에 노출되었을 경우 위험성이 커진다.
- 서비스의 특성에 따른 노출 수준이 높을수록 개인정보가 노출될 확률이 커진다.

이때 두 가지의 측도를 통해 개인정보의 노출시 발생할 위험도를 계산할 수 있다. 즉, 서비스를 통해 게시되는 정보의 노출수준(Exposure Level)과 각 개인정보의 자산가치(Property)를 고려하여 각 개인정보의 위험도(Risk Value)를 산출할 수 있고, 산출된 위험도를 사용하여 게시되는 정보에 포함된 개인정보의 개별 위험수준을 정할 수 있다. 본 논문에서는 게시되는 정보를 게시물이라 하기로 한다.

3.1 게시물의 노출수준(EL)

게시물의 노출수준은 개인정보가 게시되었을 시에 노출되는 범위의 정도이다. 개방적 구조의 서비스는 게시물의 특성에 따라 노출되는 범위가 다르다. 즉, 블로그나 게시판 등에 접근허가를 부여하는 서비스를 구현하기 때문에 이를 분석하여 보면 <표 2>와 같이 노출수준을 고려할 수 있다. 이때 부여된 EL의 값은 서비스의 접근허가 특성을 고려하여 노출수준을 구분하고 값을 지정할 수 있다. 본 논문에서는 게시판서비스에 대한 게시물의 접근허가 특성을 고려하여 노출수준을 지정하였다.

<표 2> 게시물의 특성에 따른 노출수준

EL	노출수준 설명
1	자신만이 열람할 수 있는 게시물
2	자신과 허가된 인원만이 열람할 수 있는 게시물
3	모든 사람이 열람할 수 있는 게시물

이 노출수준은 접근허가에 대한 구현이 복잡할수록 세분화하여 노출수준의 값을 지정할 수 있다.

3.2 각 개인정보의 자산가치(P)

각 개인정보의 자산가치는 개인을 식별할 수 있는 정도와 악용할 경우의 위험정도에 따라 부여된다. 각 개인정보의 자산가치는 개인정보 영향평가의 개인정보 영향도를 참조한다[8].

<표 3> 각 개인정보의 자산가치

P	조합 수준	조합 수준	조합 설명
5	P3 이상	개인을 식별할 수 있으며 악용할 경우 위험이 매우 큰 정보	주민번호, 신용정보, 신용 카드번호, 카드 비밀번호, 계좌번호, ID/PW등
	S	서비스 관련 정보	상담내용, 녹취내용, 위치정보, IP정보, CCTV 영상정보 등
4	P2+P1	개인을 식별할 수 있으며, 악용할 경우 위험이 높은 정보	-
3	P2	개인을 식별할 수 있으며, 악용할 경우 위험이 낮은 정보	이름, 주소, 전화번호, 핸드폰번호, 이메일 주소 등
2	P1	개인을 식별할 수 없으나, 개인을 식별할 수 있는 정보와 같이 노출 시 위험이 높은 정보	인종, 종교, 병역, 사회, 단체활동, 보건 등
1	G	정보가치가 낮은 정보	-

<표3>에서 제시된 것과 같이 개인정보는 정보자체가 노출될 경우 위험한 정보와 정보자체는 의미가 없지만 노출에 의해서 위험한 정보로 구분할 수 있다.

3.3 각 개인정보의 위험도(RV)

본 논문은 각 개인정보의 노출 시 위험도를 RV, 게시물의 노출정도를 EL, 각 개인정보의 자산가치를 P라고 할 때 아래 (수식1)을 통해 <표 4>와 같이 1에서 15사이 값의 위험도를 산출할 수 있다.

$$RV = EL \times P \qquad \text{(수식1)}$$

(RV: 노출 시 위험도, EL: 게시물 노출정도, P: 개인정보 자산가치)

<표 4> 위험도(RV) 산출 표

EL \ P	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15

3.4 각 개인정보의 위험수준 산정

개인정보의 개별 위험수준은 각 개인정보의 위험도에 따라 <표 5>와 같이 세 가지의 위험수준으로 분류할 수 있다. 위험 수준에서 일반적인 수준의 G(General)은 노출 시 위험정도가 낮은 수준을 의미하고 , 주의를 요하는 수준의 C(Caution)는 노출 시 개인정보를 침해할 수 있다는 것을 의미한다. 마지막으로, 위험한 수준인 D(Danger)는 개인정보 노출로 인하여 개인정보의 침해사고가 발생할 가능성이 큰 위험수준이 된다.

<표 5> 위험수준 산정 표

RV	위험수준	위험수준 설명
1-5	G(General)	해당 개인정보의 노출 시 이차 침해의 위험정도가 낮은 수준
6-9	C(Caution)	해당 개인정보의 노출 시 이차 침해의 위험정도가 높은 수준
10-15	D(Danger)	해당 개인정보의 노출 시 이차 침해의 위험정도가 매우 큰 수준

4. 위험수준 산정 방법의 적용

본 장에서는 3장에서 제시한 위험수준 산정방법을 적용하여 개인의 개인정보보호 의식수준을 향상시키고 이를 통해 이차적 침해를 예방하기 위한 게시물의 등록절차 개선안을 설명한다. 이 방법은 서비스 이용자가 게시물을 등록하는 과정에서 적용되며 서비스 이용자에게 게시물에 포함된 각 개인정보의 위험수준을 제공함으로서 서비스 이용자가 직접적으로 개인정보 보호조치를 취하도록 유도한다.

4.1 게시물 등록절차의 개선안

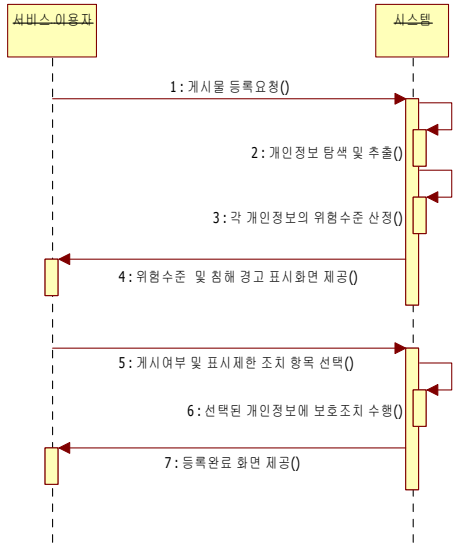
개인정보 노출을 예방하기 위한 게시물 등록절차는 (그림 1)과 같으며 3장에서 제시한 위험수준 산정 방법을 적용하여 다음과 같은 순서로 수행된다.

① 서비스 이용자는 게시물 작성 후 시스템에 등록을 요청한다.
② 시스템은 게시물에서 개인정보일 가능성이 높은 항목을 탐색하고 게시물에 개인정보가 존재하는 경우 해당 개인정보 항목들을 추출한다.
③ 시스템은 추출된 개인정보를 유형별로 분류하여 개인정보의 조합수준을 도출하고 위험수준 산정 모델에 따라 위험수준을 산출한다.
④ 시스템은 게시물에 포함된 각 개인정보와 해당 개인정보의 위험수준을 사용자에게 명시하고 위험수준에 따라 발생할 수 있는 침해 가능성을 사용자에게 경고하는 화면을 서비스 이용자에게 제공한다.
⑤ 서비스 이용자는 게시물 내의 개인정보와 각 개인정보의 위험수준을 확인하고 일정한 위험수준의 개인정보에 대하여 개인정보 표시제한 보호조치를 취할 항목들을 선택한 후 등록을 요청하거나 취소한다.
⑥ 시스템은 서비스 이용자가 표시제한 보호조치를 선택한 개인정보 항목에 표시제한 보호조치를 수행한다.
⑦ 시스템은 서비스 이용자에게 표시제한 보호조치 및 게시물 등록이 완료된 화면을 제공한다.

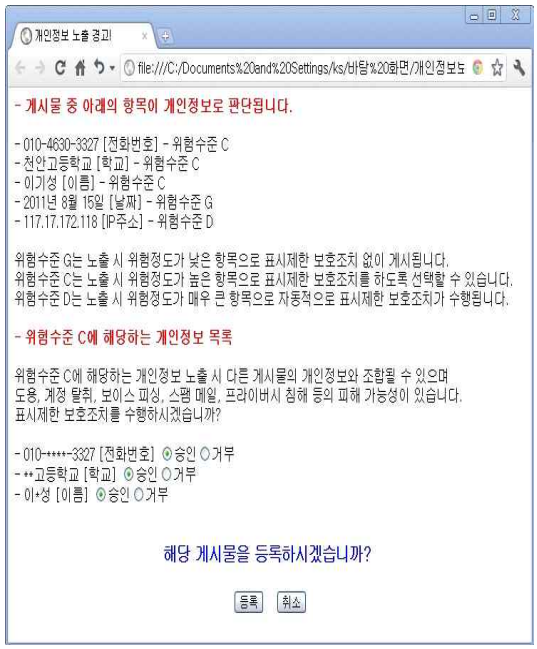
4.2 개인정보 노출 경고 표시화면 예시

개인정보 노출 경고 표시화면은 서비스 이용자에게 게시물에 포함된 개인정보와 각 개인정보의 위험수준을 제공하며 일정한 위험수준에 해당하는 개인정보에 대하여 서비스 이용자에게 표시제한 보호조치의 여부를 입력 받는다.

(그림 2)는 개인정보 노출 경고 표시화면의 예시로서 게시물의 포함된 다섯 개의 개인정보를 검출하여 각 개인정보의 위험수준을 산정하였고 위험수준 C에 해당하는 세 개의 개인정보에 대하여 표시제한 보호조치 여부를 선택하도록 하고 있으며 위험수준 D에 해당하는 두 개의 개인정보는 자동적으로 표시제한 보호조치를 취하도록 하였다. 본 예시에서 사용된 개인정보 표시제한 보호조치의 마스킹 적용규칙은 '정보통신망 이용촉진 및 정보보호 등에 관한 법률' 9조 개인정보 표시제한 보호조치의 권고사항을 참고하였다[9].



(그림 1) 게시물의 등록절차 개선안



(그림 2) 개인정보 노출 경고 표시화면 예시

서비스 이용자가 표시제한 보호조치 여부의 결정 후 게시물의 등록을 요청하면 시스템은 서비스 이용자가 선택한 항목에 대해서만 표시제한 보호조치를 취하여 게시물을 등록한다.

5. 결 론

본 논문에서는 최근 스마트 모바일 환경과 개방적 구조의 웹 2.0 환경에서의 개인정보 노출을 예방하기 위해 개별 개인정보의 위험수준을 산정하는 모델을 제시하였고 해당 모델을 적용하여 서비스 이용자에게 위험수준을 제공하고 일정한 위험수준의 개인정보는 서비스 이용자에게 보호조치 여부의 결정권을 부여하는 게시물의 등록절차 개선안을 제안하였다.

제안된 방법은 개방적 구조의 서비스 환경에서 콘텐츠 생성의 주체인 서비스 이용자에게 자신의 게시물 내의 각 개인정보의 위험수준을 제공함으로서 개인정보 노출에 대한 경각심을 일깨워 개인정보 노출을 일차적으로 예방할 수 있으며 서비스 이용자에게 일정한 위험수준을 가진 자신의 개인정보에 대한 결정권을 부여함으로서 기존의 서비스 관리자의 정책에 의한 일방향적인 개인정보보호 조치에서 벗어나 서비스 이용자가 개인정보보호를 인식하고 함께 참여하는 양 방향적 개인정보보호 문화를 만들어 나갈 수 있도록 도와준다. 이러한 서비스 이용자의 개인정보보호 의식 향상과 양 방향적인 개인정보보호 문화에 따른 일차적인 개인정보 노출 차단효과로 인하여 자연히 서비스 이용자의 직접적인 입력으로 인한 이차적인 침해사고가 감소되고 개방적 구조의 서비스 환경에서 개인의 안전한 서비스 이용이 가능할 것으로 기대된다.

본 논문에서 제시하는 위험수준의 산정 모델이 올바르게 위험수준을 산정하기 위해서는 개인정보의 정확한 식별이 필수적이다. 하지만 콘텐츠를 서비스 이용자가 생성하는 개방적 구조의 특성 상 게시물에 은어 등의 비정규적인 표현이 다수 존재할 수 있으며 이로 인하여 개인정보의 정확한 식별이 어려울 수 있으므로 개인정보 식별문제에 대한 추가적인 연구가 필요하며 텍스트만이 아닌 서비스 이용자가 게시하는 음성, 정지영상, 동영상 등 다양한 형식에도 위험성이 높은 개인정보가 포함되므로 이러한 다양한 형식에 포함된 개인정보를 식별하는 연구가 필요하다.

추가적으로 게시물 등록절차에 악성코드의 필터링 기능을 추가시켜 보안성을 강화시킬 수 있으며 게시물의 작성 시에 실시간으로 서비스 이용자에게 게시물내의 개인정보와 해당 개인정보의 위험수준을 제공하도록 설계하여 보다 효과적으로 개인정보의 노출을 예방하도록 할 수 있다.

참고문헌

[1] 한국인터넷진흥원 ISIS “개인 인터넷이용 통계” http://isis.kisa.or.kr/sub02/?pageId=020200, 2010

[2] 한국인터넷진흥원 ISIS “개인 정보보호 실태” http://isis.kisa.or.kr/sub07/?pageId=070100, 2010

[3] Pew Internet & American Life Project, "Older Adults and Social Media", Aug 27, 2010

[4] 개인정보보호종합지원시스템 “개인정보침해사례” http://www.privacy.go.kr/nns/ntc/pex/personalExam.do

[5] 손태경, “안전한 개인정보 보호방안 연구”, 숭실대학교 정보과학대학원 석사학위논문, pp. 34-36, 2011.

[6] 행정안전부 개인정보보호과 “공공기관 홈페이지 개인정보 노출방지 가이드라인”, pp. 40-42, 2011

[7] 행정안전부・한국인터넷진흥원 “공공기관 개인정보 영향평가 수행 안내서”, pp. 2-4, pp. 48-50, 2011

[8] 행정안전부・한국인터넷진흥원 “공공기관 개인정보 영향평가 수행 안내서”, pp. 31, 2011

[9] 방송통신위원회・한국인터넷진흥원 “개인정보의 기술적・관리적 보호조치 기준 해설서”, pp. 76, 2010

[저 자 소 개]

이 기 성 (Ki-Sung Lee)

2012년 공주대학교 정보통신공학과 졸업(공학사)
현재 고려대학교 정보보호대학원 재학

e-mail : hbahn@kongju.ac.kr

이수연 (Su-Youn Lee)

1990년 단국대학교 전자계산학과 (이학사)
1993년 단국대학교 전산통계학과 대학원 석사(이학석사)
2003년 성균관대학교 전기전자 및 컴퓨터공학부 대학원 박사 (공학박사)
1997년 3월 ~ 현재 백석문화대학교 인터넷정보학부 교수

e-mail : sylee@bscu.ac.kr

안효범 (Hyo-Beom Ahn)

1992년 단국대학교 전자계산학과(이학사)
1994년 단국대학교 전산통계학과 대학원 석사(이학석사)
2002년 단국대학교 전산통계학과 대학원 박사(이학박사)
1997년 9월~2005년 3월 천안공업대학 정보통신과 부교수
2005년 3월 ~ 현재 공주대학교 정보통신학부 교수

e-mail : hyobeom.ahn@gmail.com