<자연계열>

이름	수험번호

※ 발표면접은 3분 내외로 앉아서 진행합니다. 면접 시 본인의 메모를 참고할 수 있습니다.

<자료 1>은 개인정보 유출문제를 소개하고, 두 가상의 국가에서 이러한 문제에 대응하는 방법을 사례를 통해 보여주고 있다. 두 나라 대응 방법의 차이점과 장단점을 설명하고, 각각의 장단점을 고려하여 개인정보 유출과 이에 따른 피해를 줄이기 위한 보다 개선된 대처방안을 제시해 보시오.

<자료 1> 개인정보 유출과 국가별 대응방안

정보 통신 기술의 고도화로 개인의 사생활에 관련된 여러 가지 정보를 축적하여 관리하는 것이 가능해졌다. 컴퓨터에 축적된 대량의 정보는 손쉽게 검색이 가능하고 컴퓨터 통신망을 통해 전송도 용이해졌기 때문에 그만큼 사생활 침해나 정보 유출의 위험도 높아졌다. 정보를 손쉽게 획득할 수 있게 된다는 것은 그만큼 정보를 가볍게 처리해버릴 수 있는 가능성이 많아짐을 의미한다. 예를 들어 회원 전용 서비스를 위해 작성한 개인 정보가 본인도 모르는 사이에 유출되어 고액에 거래되고 이것이 단순한 사생활 침해 차원을 넘어서 범죄에까지 악용되는 경우도 있다.

국가 A에서는 이러한 개인 정보 유출 및 이에 따른 피해를 줄이기 위해 개인정보를 다루는 기관이 따라야 할 일련의 지침을 발행하고 있다. 개인을 식별 가능한 정보는 반드시 본인의 동의를 얻어 수집하여야 하며, 지정된 보관 기간 이후에는 반드시 폐기하여야 한다는 규정이 이러한 지침의 예이다. 이러한 지침을 법으로 강제함으로써 일정 수준 이상의 보안이 유지되도록 하는 효과가 있으나, 지침에 따르던 기관에서 유출사고가 발생할 경우에는 강력한 처벌이 따르지는 않으며, 따라서 피해자들에 대한 보상도 제대로 이루어지지 않고 있다.

국가 B에서는 구체적인 보안 방법의 선택을 지침을 통해 지정하거나 강제하지는 않고 개별 기관의 자율에 맡기고 있다. 하지만 유출사고가 발생하는 경우에는 강력하게 처벌하여 책임을 묻고 있으며, 피해자들에게도 충분한 보상을 하도록 하고 있다. 예를 들어 대형유통업체인 T사에서는 신용카드 정보를 포함한 개인정보 약 1억 건이 유출되었는데, 이에 따라 약 3조원 이상의 과징금을 지불하고 CEO가 사퇴하는 결과를 낳았다. 또한 모든 고객에게 1년간 무료 신용 모니터링 서비스를 제공키로 하였다. 중소기업이나 영세기업의 경우 개인정보가 유출되면 회사의 부도로 이어진다는 인식이 널리 퍼져 있다.

모의면접 해설자료 (자연계열)

출제의도

(논리 및 비판적 사고력) 개인정보유출에 의한 피해를 막기 위한 두 가지 정책 간의 차이점을 명확히 구분할 수 있는지를 평가하고, 이에 대한 대응방법을 논리적으로 제시할 수 있는지를 평가한다. (공동체의식) 또한 대응방법을 생각하는 과정에서 공동체 구성원 전체의 이익을 고려하였는지도 평가한다.

가능한 답안 예시

※ **(대응 방법의 차이점과 장단점)** 각 대응방법의 차이점에 대해 구분되게 설명하며, 한 가지 이상의 장점과 단점을 논리적으로 제시할 수 있으면 됨

- 국가 A: 각 기관이 따라야 할 구체적인 보안 규정을 가이드라인으로 내려줌. 이를 강제함으로써 최소한의 보안수준을 유지할 수 있다는 장점이 있으나, 규정을 따른 업체에서 유출사고가 발생하는 경우에는 규정에 따랐다는 이유로 처벌할 근거가 부족하다는 단점이 있음
- 국가 B: 각 기관이 따라야 할 구체적인 보안 규정이 있지는 않고 특정 방법을 강제하지도 않음. 하지만 유출사고가 발생한 경우 엄중하게 처벌을 물음. 이에 따라 대형 기관일수록 가능한 가장 강력한 보안 수단을 강구하기 위해 최선의 노력을 한다는 장점이 있음. 하지만 소규모 기업의 경우 반드시 따라야 하는 수칙이 없음으로 인해 (혹은 비용을 감당하기 힘드므로) 보안 수준이 낮아질 수 있다는 단점은 있으며, 유출 사고 발생 시 엄중한 처벌로 인해 부도를 감수해야 한다는 위험부담으로 기업 활동이 위축될 수 있음

※ **(본인이 제시한 대처방안)** 하나 이상의 해결방안을 제시하며, 이 해결방안이 개인정보 유출문제를 막기 위한 해결책으로 논리적으로 타당하여야 함. 또한 앞 문제에서 제시했던 기존 방안의 단점을 보완할 수 있는 이유를 논리적으로 설명할 수 있으면 됨

- 모든 기관에서 현재까지 일어난 개인정보유출 사례, 유출 일시, 유출된 정보의 범위, 그리고 기관에서 수행한 수습방안 등을 기관의 홈페이지에 공개하도록 의무화할 수 있음. 사용자들이 서비스업체를 선정하거나, 기관 간에 협력업체 선정 시에 이와 같은 공개된 정보를 참조할 수 있게 됨에 따라 유출이 일어난 기업은 유출 이후로도 지속적으로 손해를 보게 되므로, 보안에 더 신경 쓰게 되는 분위기를 조성할 수 있을 것임
- 개인정보보호 방법에 대한 가이드라인은 중소기업에서 참고할 수 있도록 제시하되 강제하지는 않음. 유출 사고의 피해 정도나 유출 건수에 따라 차등하여 처벌하되, 일정 수준 이상의 유출에 대해서는 엄중하게 처벌함. 자진신고하고 신속히 대응한 경우 처벌수위를 낮출 수도 있음
- 일정 크기 이상의 기관에서는 크기에 비례하여 보안 담당 팀 및 최고보안책임자(CSO)를 의무적으로 갖추도록 함
- 인터넷을 사용하는데 있어 지켜야 할 기본적인 예의와 윤리에 대한 교육을 학교, 기업에서 주기적으로 실시함으로써 개인정보를 오용·남용하는 등 다른 사용자에게 해를 끼치는 행위가 발생하지 않도록 함
- 인터넷 공간에서의 범죄는 일반 범죄보다 익명으로 이루어지기 쉬우므로 범죄 행위는 용이하나 적발이 어려워 급격하게 증가하고 있음. 따라서 인터넷 접속이 실명으로 이루어지도록 기술이나 제도를 보완할 수 있음

추가질문 예시

- 개인정보유출을 포함한 인터넷 범죄를 겪은 적이 있는가? 당시에 어떤 보상을 받았으며 어떻게 대응하였는가? 피해 이후에 인터넷 사용 방법이나 보안 개념에 있어 어떤 변화가 생겼는가?
- 인터넷에서 개인정보를 무단으로 수집하거나 오용하는 것이 왜 문제가 되는가?
- 개인정보의 오용 외에 인터넷에서 발생할 수 있는 범죄는 어떤 것이 있는가? 이를 방지하기 위해서 사용자들이 지켜야 할 윤리적 태도는 무엇인가? 인터넷의 순기능을 강화하고 역기능을 줄이기 위한 방안은 무엇인가?

평가 기준

구분	상	중	하
비판적·논리적 사고력	•두 가지 서로 다른 방안의 차이점을 체계적으로 분류 •분류에 따라 장단점을 논리적으로 제시 •두 방안에 각각에 대해 장점과 단점을 하나 이상씩 제시 가능 •남들과는 다른 관점에서 문제를 생각해보고 대처 방안을 제시할 수 있음 •제시한 대처 방안이 논리적으로 타당함	•두 방안에 대한 차이점이 체계적으로 분류되지 않고, 자료의 내용을 단지 요약하여 차례로 설명함 •주장이 논리적으로 전개되나 논리 자체가 단순하거나 설득력이 부족함 •주어진 논쟁의 요점을 대략적으로 또는 부분적으로 이해 •이미 널리 알려진 관점이나 해결방안을 약간 변형하여 제시	•주어진 제시문을 대부분 이해하지 못함 •합리적 추론에 바탕을 두지 않은 억지스런 주장을 펼침 •주제와 크게 연관이 없는 의견을 제시 •제시문에 주어진 내용만을 언급
인성(공동체 의식)	•대처방안을 제시하는데 있어 공동체 구성원 다수의 이익을 고려하였으며, 실현 가능한 방안을 구체적으로 제시	•제시한 대처 방안이 많은 사람에게 도움이 될 수 있는 이유가 충분하지 않음 •주어진 문제를 해결하고자 하는 의지나 진정성이 부족해 보임	•공동체를 고려하기보다는 개인적인 관점에만 기반하여 답안을 제시

자료출처 (아래 본문의 내용을 참고하여 재구성함)

도서명(출판사)	페이지/링크	내 용
생활과윤리(교학사)	p.165-168	정보통신기술과 윤리문제
정보통신일반(교학사)	p.38-39	정보 사회의 변화와 윤리
개인정보보호지침	인터넷진흥원 개인정보보호 관련 자료실 http://privacy.kisa.or.kr	
보안뉴스	[글로벌 개인정보보호] 개인정보 유출 제재사례 http://www.boannews.com	