제28회 한국정보처리학회 추계학술발표대회 논문집 제14권 제2호 (2007. 11)

재난관리시스템의 개인정보보호 취약성 분석

정진호 [o*], 김현석[**], 김주배[**], 최진영[**]
[o*]고려대학교 디지털정보공학과, [**]고려대학교 컴퓨터학과
e-mail : [*]jhpoadm@nema.go.kr, [**]{hskim, jbkim,choi}@formal.korea.ac.kr

The Vulnerability Analysis of the Personal Privacy Security in the Disaster Management System

Jin-Ho Jeung[*], Hyun-Seok Kim[**], Ju-Bae Kim[**], Jin-Young Choi[**]
[*]Dept of Digital Information Technology, Korea University
[**]Dept of Computer Science, Korea University

요 약

국가 재난관리 시스템(National Disaster Management System: NDMS)은 개발 및 운용상의 여러 이유로 인해 개인정보의 수집을 필요로 한다. 그러나 이렇게 수집된 개인정보는 수집단계에서부터 소멸단계까지 인가/비인가 관리자에 의한 악용 또는 침해우려가 높다.
본 논문에서는 이러한 개인정보들의 관리 및 보호를 위해 재난관리시스템을 대상으로 보호대상 개인정보를 분석하고, 도출된 개인정보에 대하여 재난관리 업무상의 보호/통제를 평가하며, 개인정보 Life Cycle 별 위협 요소 및 잠재 위험 분석을 통한 영향평가를 수행하여 개인정보보호를 위한 관리적, 기술적, 물리적 대응방안을 제시하고자 한다.

1. 서론

정보사회의 눈부신 발전에 따라 정보시스템이 우리에게 주는 긍정적 이점에 반하여 부정적 영향 또한 증가하고 있다. 날로 심각해지는 개인정보 침해 문제는 최근 많은 논란 속에 정보보호 분야의 이슈로 떠오르고 있는 부문이다. 이에 따라 국내외 주요기관에서는 개인정보보호 관련 법률/지침[6]에서 '개인정보(PI: Private Information)' [7][8]개념을 정의하고 개인정보보호를 위한 노력을 지속적으로 추진하여 왔다.

현재까지는 시스템 구축 이후에 접근금지 및 침입방지 등의 방법으로 보호하는 정책을 가져왔던 것이 현실이지만, 시스템 개발 단계에서부터 개인정보보호에 대한 근거 및 기준을 마련하고 각 단위시스템이 마련된 규칙에 준하는지에 대한 통제 및 해당 시스템의 정보특성에 따른 보다 구체적인 보호 대책이 더욱 중요하다 하겠다.

집중호우, 태풍 등의 자연재해 및 건물의 붕괴, 지하철 사고 등 인적 재난 발생 시에 그 피해를 최소화하기 위한 각종활동을 지원하는 재난관리 정보시스템은 전국의 피해상황을 집계하고 복구활동을 지원하기 위해 국민의 각종 개인정보를 취합하고 관리한다. 이러한 재난관리 정보시스템의 개인정보가 유출되어 부정적 목적으로 사용된다면 재난으로 인한 피해 이상의 심각한 물질적 정신적 피해를 야기할 수 있다.

이러한 위험요소의 분석 및 관리를 위한 본 논문의 구성은 다음과 같다. 제 2 장에서는 기존 사례 중 교육행정정보시스템(NEIS)의 개인정보보호 미비에 대한 관련 연구 및 이를 위한 개인정보보호 영향평가의 개념에 대해 소개하고 제 3 장에서는 재난관리시스템에서의 개인정보관리에 대한 분석을 기술하며, 제 4 장에서는 이러한 재난관리 시스템에서 개인정보 영향평

가를 통한 보호대책을 소개한다. 마지막으로 제 5 장에서는 결론 및 향후 개인정보보호 대책의 나아갈 방향에 대해 기술한다.

2. 관련연구

2.1 개인정보보호 영향평가제도의 배경[5]

지난 2003 년 교육 행정정보시스템(NEIS)의 개인정보침해 등 정보보호 인식 부족 및 정보이용에 대한 사전 합의 미비로 NEIS 는 개인정보침해에 대한 사전 합의 및 유출가능성에 대한 충분히 반영되지 못해 재개통에 3 년 소모, 추가비용 등 발생했으며, 전자정부 민원서비스의 문서 위변조 가능성에 대한 정보 위변조 방지 등 정보보호 측면의 기능 구현 미흡이라는 민원이 제기되었다. 이러한 과정에서 전자정부 민원발급 문서의 위변조 가능성 제기로 서비스가 1.5 개월 중단되어 사회적 손실 비용 또한 발생하게 되었다. 이러한 NEIS 를 둘러싼 논쟁을 계기로 많은 관심을 받게 된 개인정보영향평가의 필요성은 우리 사회의 정보보호와 정보인권의 향상에 많은 진보를 이룩하였다. NEIS 와 같은 대규모 사업이 초래할 사회적 위험성과 예산 낭비를 방지하기 위한 방안의 하나로 다양한 영향평가가 제안되고 있다. 그 중에 어떤 사업이 개인정보에 관한 권리에 미치는 영향을 사전에 측정하고, 부작용을 경감시키거나 피하기 위한 방법을 결정하기 위한 과정이 개인정보영향평가다.

2.2 개인정보보호 영향평가제도의 이해

개인정보보호 영향평가(Privacy Impact Assessment)[1]란 새로운 정보시스템 도입이나 개인정보 수집에 앞서 시스템의 구축 운영이 고객, 국민의 프라이버시에 미치는 영향을 평가하는 체계적인 절차를 의미한다. 이러한 개인정보보호 영향평가는 단순한 시스템 평가 차원을 넘어 사업시행으로 인해 개인정보에 미칠 수 있는 중대한 영향을 사전적으로 고려하는 것이며, 최근 여러 나라에서도 IT 시스템 도입시 반드시 고려해야 할 사항으로 명시하는 등 그 중요성은 이미 국내외에 모두 인지되어 있는 상황이다. 이는 구축되기 이전 단계에서 제안된 정보시스템에 대하여 분석하는 절차를 의미하는 계획적, 컨설팅적 측면이 강한 조치라고 할 수 있지만, 최근에는 기존 서비스 운영 중에라도 개인정보의 수집, 이용 및 관리상에 중대한 침해 위험이 발생할 가능성이 있다면 개인정보보호 영향평가를 수행하도록 권장하고 있는 추세이다.

과거 NEIS 시행에 따른 진통을 보면 교육현장과 행정을 전산화 하여 발전시키고 효율화 하자는 의도가 있었음에도 불구하고, 프라이버시 침해 등의 문제로 심각한 장애에 직면하여 개인정보 관련 침해 문제가 사전 해결되지 않은 사업추진은 전자정부 발전에 걸림돌이 된다는 교훈을 여실히 보여준 사례라고 할 수 있다. 이와 같이 최근에는 각 기관이 개인정보 자료를 수집하고 축적하는 정보시스템에 대하여 신규 혹은 기존시스템 모두 개인정보보호에 미칠 영향에 대한 조사, 예측, 평가하고 대응책을 마련할 필요성이 증대되고 있다.

2.3 개인정보보호 영향평가 수행절차

개인정보보호 영향평가는 개인정보 보호 요건분석, 보호대상 개인정보 분석, 개인정보 영향평가, 개선방안 수립의 4 단계로 구분되어 수행되고 있으며, 내용은 다음과 같다.

<표 1> 개인정보 영향평가 수행절차[6]

개인정보 보호 요건분석	1.1 개인정보보호 법/제도 분석 - 공공기관 개인정보보호에 관한 법률/시행령/시행규칙 - 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 통신비밀보호법 - 개인정보보호 기술적/관리적 보호 조치 기준
	1.2 개인정보보호 동향 분석 - OECD 개인정보보호 지침 - APEC Privacy Framework 등
보호대상 개인정보 분석	2.1 업무 기능/프로세스 분석
	2.2 정보시스템 현황 분석 - 정보시스템 및 IT 인프라 분석 - 업무기능/정보시스템 상관분석 - 데이터 흐름 분석
	2.3 개인정보 범위 정의 및 분류 - 보호대상 개인정보 범위 결정 - 개인정보의 식별/유형 분류 - 개인정보 등급(중요도) 분류
	2.4 개인정보 취급 현황 분석 - 개인정보 작성/사용 패턴분석 - 개인정보 Life-Cycle 별 개인정보 취급현황 분석
개인정보 영향평가	3.1 개인정보 통제평가 - 업무상 개인정보 보호 통제평가
	3.2 개인정보 위험 분석 - 개인정보 Life-Cycle 별 보안 위협 요소 분석 - 개인정보 잠재위험 평가
개선방안 수립	4.1 잠재위험별 개선 방향 결정 - Cost-Benefit 을 고려하여 개인정보 보호를 위한 관리적/기술적/물리적 대응방안 수립

3. 재난관리 정보시스템의 개인정보관리에 대한 분석

국가재난관리 정보시스템(National Disaster Management System: NDMS)[2]은 재난관리 관계기관에서 활용하는 시스템으로 각종 재난 발생정보와 함께 응급조치, 피해집계, 복구, 이재민관리 등을 처리하고

있다. NDMS 에서 개인정보가 포함되어 있는 현황은 다음과 같다.

<표 2> NDMS 의 개인정보가 포함된 단위시스템[2]

피해 상황 관리	- 인명, 사유시설, 선박 피해 - 각종 자연재난 발생에 대한 피해를 구분하여 피해유형/피해액 공식 집계
이재민 관리	- 이재민관리, 구호비 지급내역 - 재난발생지역의 이재민 수용현황, 구호비 지급현황 등 관리
복구 관리	- 주택/사유시설 복구, 인명피해보상 - 재난 피해발생에 대한 복구비 산정, 국비/지방비 지원

재난관리 정보시스템에서 다루고 있는 개인정보의 범위는 개인식별정보와 재난피해정보 및 복구정보가 포함되는 개인 재난관련 정보로 구분할 수 있다.

<표 3> NDMS 의 개인정보 범위[2]

개인정보	개인식별정보	개인속성정보 (일반인)	이름, 성별, 주민등록번호, 세대주 여부, 외국인여부, 군인여부, 주소, 나이
		개인속성정보 (재난관리자)	이름, 소속, 전화번호, 이동전화번호, 주소, 담당업무, 담당부서명
	개인재난관련정보	인명피해정보	사망여부, 부상여부, 실종여부, 병원명
		재산피해정보	피해재산, 피해물량, 피해금액
		이재민정보	이재민 여부, 구호비 지급 은행명, 계좌번호, 구호비 지급내역
		복구정보	복구대상여부, 지원금 수령여부, 복구지원 금액, 수령금액

4. 재난관리 시스템에서 개인정보 영향평가를 통한 보호대책

소방방재청 및 각 지방자치단체에서 취급하고 있는 재난관리 정보는 재난발생과 더불어 개인피해내역, 이재민내역, 복구내역, 재난관리 담당자정보와 같이 분류할 수 있다. 그리고, 국가재난관리 정보시스템 사용에 대한 각 경로에서 유출된 개인정보에 대한 잠재 위험/보호대책은 개인정보 작성단계(피해조사서), 개인정보 사용단계(관계기관), 개인정보 저장/관리단계(국가재난관리 정보시스템), 개인정보 폐기단계로 구분되며, 이에 내용은 <표 4>[3]와 같다. 또한 <표 5,6,7> 에서는 NDMS 의 관리적, 기술적, 물리적 측면에서 이러한 잠재위험으로 인한 개인정보보호 대책들을 기술하고 있다.

<표 4> NDMS 의 각 단계별 개인정보 잠재위험

구 분	잠재위험 (Potential Risk)
개인정보 작성단계	- 불필요하거나 민감한 개인정보 입력 - 다양한 웹 해킹 공격의 시도 (키보드 해킹, 전송데이터 스나핑 등)
개인정보 사용단계	- 사용자 인증 시, 우회 접속으로 인해 개인정보 도용 피해 - 암호화되지 않은 데이터 전송 시, 사용자 계정정보, 개인정보 유출 - 시스템 상에서 개인정보 조회 시, 안전한 사용자 인증 절차 미흡 - 화면캡처, 출력 혹은 이동형 저장매체의 사용 통제의 미비로 인한 개인 정보유출 - 개인정보에 대한 권한 통제의 미비로 취급자에 의한 불필요한 정보접근 및 외부 유출
개인정보 저장 및 관리단계	- 개인정보의 임시파일 저장 시 유출 - 게시판 등에 불필요한 개인정보 기재
개인정보 폐기단계	- 과거 피해조사서에서 작성한 개인정보가 계속해서 관리될 위험

<표 5> NDMS 의 각 단계별 관리적 측면에서의 개인정보 보호대책

구 분	보호대책 (Safeguards)
개인정보 작성단계	- 웹사이트의 기술적 취약점 제거 (응용시스템 보안 가이드라인 적용) - 불필요한 개인정보 수집 제한 - 키보드 입력보안, SSL 통신
개인정보 사용단계	- 국가재난관리 정보시스템 사용자 계정관리를 위한 기본통제 - 공인 인증서 또는 민원인의 고유 비밀정보 질의를 통한 사용자 인증 - 주요 통신 구간의 데이터 암호 전송 - E-Mail/SMS 에 의한 사건관련 통지 - 개인정보 조회 시, 관리자 확인용 추가정보 질의/응답 기능 적용 - 웹 화면의 출력기능의 제한 등의 출력 보안 적용(DRM) - 접근범위 및 권한 통제에 대한 권한 분리 등의 기본통제
개인정보 저장 및 관리단계	- 개인정보 DB 접근통제 및 암호화 - 개인정보 취급자 PC 공유폴더 금지 - 구글 검색엔진에 의한 개인정보 차단을 위한 통제 - 피싱이나 E-Mail 도용을 통한 개인정보의 유출 방지

개인정보 폐기단계	- 과거 개인정보 등급별 사용 제한

위의 잠재위험과 보호대책을 고려하여 각 단계별 개인정보보호를 위한 시스템 구축 방향을 다음과 같이 제시한다.

<표 6> NDMS 의 개인정보보호를 위한 기술적 개인정보 보호대책

구 분	설 명
키보드 보안	- 키보드 해킹 차단 (1 차적용)
웹 어플리케이션 방화벽	- 웹 어플리케이션 해킹/바이러스/웜 방지
웹 페이지 보안	- 화면캡처, Copy & Paste, 소스보기, 인쇄/전송 - 화면출력 개인정보 제한
웹 구간 암호화 (SSL)	- 전송 정보의 비인가 노출방지
SSO 권한관리	- 사용자 인증 및 권한 관리
DB 접근제어/ 암호화	- 파일 업로드, 다운로드 통제 - DB 에서의 개인정보 암호화
서버 접근제어	- 비인가자의 정보 접근 통제
보안감사추적	- 주요 개인정보 접근/열람 기록의 관리
개인정보관리 인프라 운영	- 정보보안 및 개인정보보호 정책/지침 설계 및 구축 - 개인정보 식별 및 등급 관리 - Off-line 유통문서의 보호

<표 6> NDMS 의 개인정보보호를 위한 물리적 개인정보 보호대책

구 분	설 명
1. 피해조사서 이용	이를 바탕으로 개인정보 생성시 사용자 PC 키로깅, 바이러스로부터 보호 및 불필요한 개인정보 수집 제한
2. 통신방식 (전송 및 조회시)	전송 및 조회단계에서는 전송 데이터를 암호화하며, 안전한 통신방식을 적용. 또한 소방방재청 및 시.도, 시.군.구에서 피해집계 및 상세 정보를 조회할 경우 SSO, EAM 등의 안전한 사용자 인증 및 사용자 분류를 통한 권한관리로 정보 접근을 제한
3. 로그기록 (저장시)	시스템 운영자, DBA, DBMS 취약점에 의한 대량 개인정보 유출을 예방, 중요 정보의 경우 암호화를 통한 저장방식을 이용. 그리고 LOG 등 정보사용에 대한 접근 사용기록을 저장, 정보 수정 및 삭제에 대한 추적의 가능성 높임
4. 관리 지침 운영 (관리시)	"정보보안 및 개인정보 보호 정책" 및 "개인정보보호 관리지침" 등의 구축 및 운영을 통하여 사전에 개인정보 유출에 대한 방지, 개인정보 식별 및 등급관리, 보안시스템 구축 및 운영, 정보저장 매체 통제 등을 통하여 개인정보를 관리

5. 결론 및 향후 연구방향

본 논문은 국가재난관리 시스템의 개발 과정에서 해당시스템의 정보특성에 따라 개인정보 침해사고 발생 가능성에 대한 별도의 개인정보 영향평가를 도입하여 정보보호 효과를 극대화 할 수 있는 방안을 관리적, 기술적, 물리적 측면에서 제시한다. 특히, 공공부문의 정보시스템은 체계적이고 상대적으로 매우 정확한 개인정보를 대상으로 하는 경우가 많아 정보보호에 대한 적극적인 대응이 필요하다. 이러한 개인정보 영향평가제도 연구를 통해 프라이버시 문제를 사전에 발견하여 정보시스템의 구축 운영에 있어 시행착오를 예방하고, 효과적인 대응책의 수립을 가능하게 하여 프라이버시에 관하여 국민의 불만 등 외부개입 이전에 내부적으로 문제를 파악하고 처리하여 기관에 대한 신뢰 증진시킬 수 있으며, 개인정보 영향평가수행을 통하여 기업 내 개인정보보호에 대한 인식제고 및 전문인력 양성 등의 파급 효과도 기대할 수 있다. 향후 관련 연구방향은 본 연구에서 제시한 개인정보보호를 위한 구축방향에 대한 세부적인 사항들을 보다 기술적인 부분에 초점을 맞추어 연구를 진행하고자 한다.

참고문헌

[1] 정보통신부, "기업의 개인정보 영향평가 수행을 위한 가이드, 2005.12
[2] 이재은 김겸훈, "재난관리 정보공유와 NDM 의 실태분석 및 개선방안" 2005.12
[3] 김동규, "우리나라 재난관리체계의 개선방안에 관한 연구" 2004.8
[4] 정현백, "디지털 프라이버시와 공공부문의 정보관리" 연세행정논총 제 29 집
[5] 김영환, "정보화 사회에서 개인정보보호에 관한 연구" 2002
[6] 유희일 임명복, "정보화 사회에 있어서 개인정보 침해에 대한 법적 구제" 2002
[7] Cady, Glee Harrah & McGregor, Pat 2002. Protect Your Digital Privacy: Survival Skills for the information Age. New York: Que.
[8] Erbschloe, Michael & Vacca, John 2001. Net Privacy. New York; McGraw-Hill.