국가R&D정보관리 환경에서 ISO 27001(ISMS) 성과 및 개선 방향

이병희*, 여일연*, 김재수*
*한국과학기술정보연구원 NTIS사업단
e-mail: {bhlee, ilyeon9, jaesoo}@kisti.re.kr

Outcome and Enhancement of ISO 27001(ISMS) in National R&D Information Management Environment

Byeong-Hee Lee*, Il-Yeon Yeo*, Jae-Soo Kim*
*NTIS Division, Korea Institute of Science and Technology Information

요 약

R&D에 관한 주요 국가 및 산업기술의 정보 유출이 문제가 되고 있다. 2009년 11월 국가과학기술지식정보서비스(NTIS)는 영국표준협회(BSI)로부터 ISO 27001에 대한 11개 도메인, 133개 보안 통제항목의 정보보호관리체계((Information Security Management System) 인증을 획득하였고 이후 사후인증 심사를 받고 있다. 본 논문에서는 정보보호 국제 표준인증인 ISO 27001과 관련하여 NTIS의 정보보호관리체계에 대하여 국가R&D정보관리의 경영적 관점에서 실증적 현황 및 성과와 향후 개선 및 발전 방향에 대하여 검토한다. ISO 27001 도입 후 133개 통제항목 중에서 적용율이 증가하였고 중부적합/경부적합/개선권고 사항이 크게 감소하였으나 정보자산 및 개인정보 관리는 지속적인 관심과 개선이 필요함을 알 수 있었다.

1. 서론

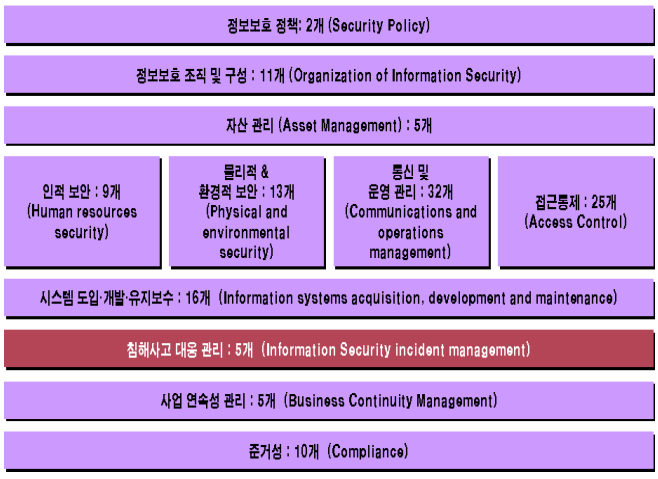
최근 R&D에 관한 주요 국가 및 산업기술의 정보 유출이 심각한 사회적 이슈로 등장하였다. 2008년 3월말 국가R&D정보의 지식 포털인 국가과학기술지식정보서비스(NTIS)가 대국민 서비스가 오픈되고 NTIS의 주요 6개 서비스가 개시되었다. 이를 위해 NTIS는 운영·지원·모니터링에 대해 NTIS 표준운영절차(SOP)를 수립하고 2008년 10월 국제표준인 ISO 20000(IT 서비스관리) 인증을 받아 그 절차에 따라 안전하게 운영·관리되고 있다.

NTIS의 각 서비스에 대한 사용자 권한 제어를 통해 데이터의 불법 접근을 차단하고 최근 나날이 고도화·지능화되고 있는 각종 해킹에 능동적으로 대처하기 위해 정보보안에 대한 지속적인 검토 및 보완이 요구된다. 이런 상황에서 NTIS 서비스에 대한 고객의 신뢰도를 확보하기 위해 NTIS 정보자산을 내·외부 위협으로부터 보호하기 위한 정보보호 관리체계의 국제표준인 ISO 27001 관리체계 도입 필요성이 제기되었다.

본 논문에서는 2009년 11월 ISO 27001 인증을 획득하고 현재까지 관리하고 있는 NTIS의 ISO 27001에 대하여 국가R&D정보관리의 경영적 관점에서 실증적인 추진 현황 및 성과, 향후 개선 및 발전 방향에 대하여 알아보고자 한다.

2. 관련 연구

국내에서 정보시스템을 운영하고 있는 기업이나 기관들에서 체계적인 위험분석 및 보안관리에 대한 요구가 늘어나고 있다. 이러한 요구에 부합하여 나온 국제표준 규격이 ISO 27001이다[1].



(그림 1) ISO 27001의 구성

ISO 27001은 비즈니스 위험에 대비하여 정보보호에 대한 계획, 구현, 운영, 검토 및 개선을 위한 조직체계 및

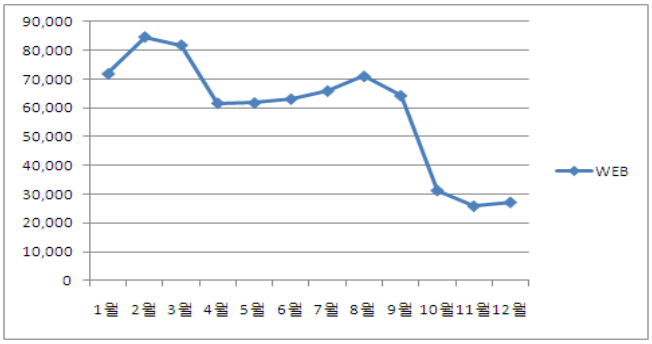
정책, 정보보호 프로세스 및 절차, 지침 등으로 구성된 정보보호관리체계(Information Security Management System, ISMS)로 (그림 1)과 같이 11개 보안 도메인과 133개의 보안 통제항목(인증심사 항목)으로 구성된다.

[2]에서는 국제적인 정보보호관리체계의 표준화 동향에 대해 조사, 분석하여 정보자산에 대해 통합적으로 위험을 관리할 수 있는 정보보호관리시스템을 제안하였다. 하지만 보안성숙도 측정 모델링에 머물러 실질적인 적용사례 연구에는 미흡하다. [3]에서는 중앙행정기관 및 지방자치단체에서 제공하고 있는 전자정부 서비스의 안정성과 보안성을 향상시킬 수 있는 정책을 발굴하여 국가 정보보호 수준을 높이고자 하였다. [4],[5]에서는 NTIS의 ISO 27001 적용의 초창기 체계 수립에 머물렀다.

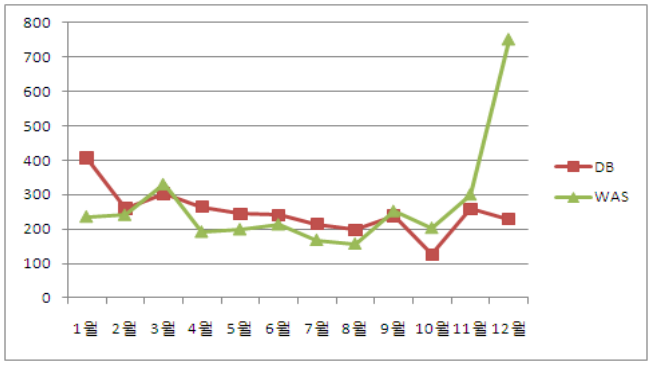
본 논문에서는 NTIS의 ISO 27001 인증 이후 최근 3년간의 적용 경험을 바탕으로 경영의 관점에서 실증적 현황 및 성과와 향후 개선 및 발전방향에 대하여 검토하고자 한다.

3. NTIS의 ISO 27001 현황 및 성과

NTIS 서비스에 대한 월별 침입탐지 수를 2009년을 예를 들면 아래와 같이 그 수가 상당하다. (그림 2)와 (그림3)은 웹/DB/WAS의 월별 침입탐지 수이다.



(그림 2) NTIS 웹 월별 침입탐지 수



(그림 3) NTIS DB/WAS 월별 침입탐지 수

특히 NTIS의 여러 주요 서비스에는 다음과 같은 위협이 있다. NTIS의 국가R&D사업관리서비스는 1993년부터 2009년까지의 국가R&D 관련 과제, 성과 및 연구자의 개인정보·제재정보가 구축되어 있어 데이터의 누출 시 오·남용으로 피해가 클 것으로 예상된다. 또한 NTIS의 과학기술인력정보서비스도 2006년 이후 현재까지의 과학기술인력 개인정보가 구축되어 데이터의 오·남용 및 유출 시 피해와 부작용이 클 것으로 판단하고 있다. 또한 NTIS의 웹 콘텐츠의 복사, 저장, 인쇄 기능을 이용한 통계 및 분석 정보의 대량 복제가 가능하며 이에 대한 보완(DRM 포함)이 필요하다. 이외에도 NTIS의 각 서비스에 대한 사용자 권한 제어를 통해 데이터의 불법 접근을 차단하고 최근 나날이 고도화·지능화되고 있는 각종 해킹에 능동적으로 대처하기 위해 정보보안에 대한 지속적인 검토 및 보완이 요구되었다.

이런 환경에서 2008년 3월말 대국민 서비스를 시작한 NTIS는 NTIS의 각종 정보자산 및 서비스를 각종 위협으로부터 보호하고 관리하기 위하여 ISO 27001 인증을 도입하기로 하였다. 이를 위해 기존에 표준운영절차(SOP) 및 2008년 10월에 인증을 받은 ISO 20000과 유기적으로 연계하여 NTIS는 국제규격을 준수한 정보보호관리체계를 구축하고자 하였다.

이해 관계자로는 국가정보원, 교육과학기술부(주요 고객, 2011년 3월말 국가과학기술위원회 업무로 이전), 행정안전부, NTIS서비스 대상 고객 등이며 국가정보원, 교육과학기술부, 행정안전부 등의 보안평가가 매년 있다. 준수하고 있는 법규 및 규정으로는 국가정보보안 기본지침(국가정보원), 교육기관 정보보안 기본지침(교육과학기술부)과 기관 및 조직 내부 정보보호 규정 및 지침 등을 고려하였다.

<표 1>은 최근 3년간 영국표준협회로부터 받은 부적합 및 개선권고사항 수이다. 괄호 안의 수는 내부심사에서 받은 수이다.

<표 1> 부적합 및 개선권고사항 비교

연도	중부적합수	경부적합수	개선권고수
2009	0(2)	1(19)	17(7)
2010	0(1)	0(11)	11(12)
2011	(0)	(0)	(8)

인증 받은 이후 다음과 같은 성과나 변화가 있었다.

- 보다 객관적으로 조직에 맞는 KPI로 변화. 2009년 대비 2010년 통제항목(133개) 적용율이 75%(100개)에서 79%(105개)로 향상됨
- “내PC지키미” 프로그램의 전체 PC 적용 및 상주 용역업체로 확대 적용됨
- 네트워크 접근통제 제도(NACAgent, 내PC지키미, V3(IS8.0), PMS, VMS)를 설치/적용해야 함) 전면시행과 USB 보안관리 체계 도입
- 조직내에 보안 프린터/복사기 도입
- 서비스에 DRM 적용(사업관리/인력 서비스에 선 적용 후 확대예정)
- 조직내 정보자산관리 강화

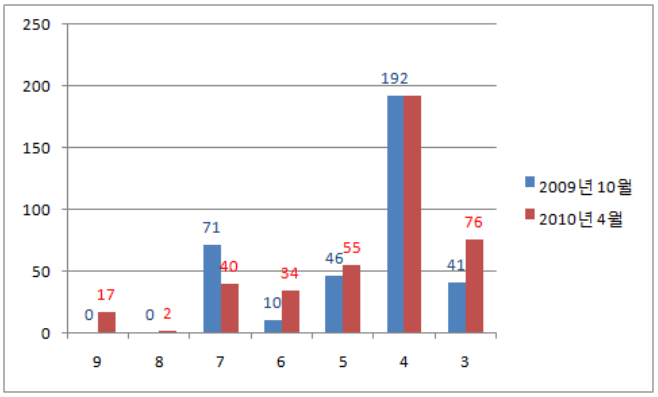
이외에도 정성적인 성과로는 보안의식 증진과 보안교육 강화 등이 있으며, 국가정보원 같은 외부기관으로부터의 보안신뢰성 평가 향상이 이루어 진 점이 높이 평가된다.

4. NTIS의 ISO 27001 향후 개선 및 발전 방향

최초 인증시인 2009년과 비교하여 부적합 및 개선권고 사항 수가 줄어들고 있으나 아직 개선할 내용이 있으며 지속적인 관심과 실행이 필요하다.

특히, 정보자산관리를 위해 아래와 같은 노력이 필요하다.

- 정보자산조사에서 일부 누락된 자산을 발견하여 자산조사에 신규자산으로 포함하였음. 정확한 정보자산조사가 관리될 수 있는 체계 및 사용자 각자의 협조가 필요하다.
- 2009년 조사된 자산에 대해서는 DOA(레벨 7)이상의 위험도를 가지는 자산에 대해 조치가 이루어졌으나, 2010년 1차 자산조사에서 아래 (그림 4)와 같이 레벨 7이상의 위험도를 가지는 자산도 발견되는 경우도 있었다.



(그림 4) 최고 위험도(C, I, A 위험도중 최고치)별 자산 분포, (X축:위험도, Y축:자산수)

매년 신규 자산이 추가되거나 폐기 처분도 고려해야 하나 PC의 경우 폐기 처분이 제대로 이루어지지 않는 부분도 있다. 향후 위험도를 줄이기 위한 활동이 보다 계획적이고 효율적으로 진행되도록 개선해야 하며, 조치 활동에 대한 취약 정도의 변경에 대한 구체적인 기준을 마련하여 평가가 객관적으로 이루어지도록 해야 할 필요가 있다.

향후 ISO 27001과 관련하여 아래와 같은 개선 및 발전 방향이 필요하다.

- 노트북 수리시 보안성, 기밀성 확보방안 검토
- PC 폐기 시 NTIS 보안담당자 입회절차 수립/적용 검토
- 정보자산을 용도별로 그룹핑하여 관리 및 위험도 평가 검토
- 보안관련 법규와 정부 행정망(교육과학기술부, 지식경제부 등) 보안적용을 모니터링하여 해당되는 부분은 적극 검토
- 현재 법규 준수여부 평가가 포괄적임. 향후 세부 레벨로 준수여부 파악 검토
- NTIS의 주기별(월별/주별/시간대별) 정보 침입 탐지/차단 통계집계가 가능하도록 검토할 것
- 공공기관 부문 정보보호대상 조사 및 검토
- 개인정보보호 방안 검토. NTIS의 개인정보자료[NTIS 고객(회원) 정보<통합홈페이지>, 과제참여인력<SIMS>, 연구자 및 평가위원Pool, 장비·기자재 전문가Pool 등], 사용자 유형 및 권한관리(2010.2월 국정원 요청자료)와 주민등록번호 사용 제한, 기타 개인 PC에 저장된 개인정보(15개 부처청 및 대표전문관리기관 연락처, NTIS 평가위원 등)의 철저한 관리 등이 필요하다.

5. 결론

본 논문에서는 정보보호 국제 표준인증인 ISO 27001과 관련하여 NTIS의 정보보호관리체계에 대하여 국가R&D정보관리의 경영적 관점에서 실증적 현황 및 성과와 향후 개선 및 발전 방향에 대하여 검토하였다. ISO 27001 도입 후 133개 통제항목 중에서 적용율이 증가하고 중부적합/경부적합/개선권고 사항이 크게 감소하는 성과가 있었으나 향후 정보자산관리와 개인정보보호는 지속적인 노력이 필요함을 알 수 있었다.

ISO 27001 인증으로 NTIS는 참여 부처와 행정효율화 도모는 물론, 범 부처 차원에서 서비스 신뢰성이 크게 제고될 것으로 기대된다. 향후 NTIS는 범 부처와 유기적으로 협력하여 지속적으로 서비스 수준을 관리하고 정보보호체계를 강화하여 궁극적으로 고객(국민) 만족도를 향상시킬 수 있도록 노력할 계획이다.

참고문헌

[1] ISO 27001:2005 Information security management system specification
[2] 김태달, “ISO 27001의 ISMS 보안성숙도 측정 모델링에 관한 연구- ISO 27004 정보보호관리 측정 및 척도체계”, 한국컴퓨터정보학회, Vol.12, No.6, pp.153-160, 2007.
[3] 한근희, “전자정부 정보보호관리체계(G-ISMS) 적용정책”, 정보보호학회논문지, Vol.19, No.5, pp.119-130, 2009.
[4] 이병희, 정옥남, 김재수, “국가과학기술종합정보서비스의 ISO 20000 프로세스 설계와 체계 수립”, 한국기술혁신학회 추계학술대회, pp.79-89, 2008.11.
[5] 이병희, 임철수, 신동구, 정옥남, 김재수, "NTIS의 ISO 27001 체계 수립과 ISO 20000 인증 사후관리", 한국기술혁신학회 추계학술대회, pp.373-380, 2009.11.
[6] 이병희, “NTIS ISO 27001 경영검토보고서” 2009.10.
[7] 이병희, “NTIS ISO 27001 경영검토보고서” 2010.5.