"국민에게 신뢰받는 최고의 국토정보 전문기관"

성과감사

한국국토정보공사 본사

2015년 성과감사 결과보고서

2015. 9.

감 사 실
한국국토정보공사

Ⅰ. 감사실시 개요

□ 감사 배경

○ 공사에서는 2013년부터 IT 보안관련 자원의 활용이 가속화되고 있으나, 그 동안의 감사는 일반 운영시스템 활용도 위주의 점검으로 이행되어 효과적인 운영과 최상의 보안을 위해 IT부문의 보안 현황에 대한 점검의 필요성이 대두되고 있다.

○ 이에 따라 공사 주요 정보보안 정책의 적정성 및 운영의 효율성 등을 진단해 보안 취약점을 개선함으로써 국토정보 대국민 서비스가 강화되도록 보안정책에 대한 진단을 실시하였다.

□ 감사 목적

○ 이번 감사에서는 공사가 현재 도입·운영하고 있는 보안정책 및 시스템에 대하여 문제점을 식별하고, 개선안을 제시함으로써 업무환경을 향상시키고 공사 보안 환경에도 변화를 추진하는데 그 목적이 있다.

□ 감사 범위

○ 감사의 범위는 본사 △△△△처 등 총 4개 부서를 대상으로 내부 보안규정과 보안절차(지침)를 점검하는 것으로 선정하였으며, 감사 시점에서 불합리한 정책과 비효율적으로 운영되는 보안업무 부문을 감사하였다.

□ 감사방법 및 절차

○ 보안규정 및 시스템 그리고 외부용역의 관점 3개 항목으로 분류하고 각 항목별 진단을 수행하여 개선(안)을 마련하는데 중점을 두었다.

□ 감사기간 및 인원

○ 2015. 8. 31. 부터 같은 해 9. 4. 까지 5일간 2명의 감사인력(연인원 10명)을 투입하여 실지감사를 수행하였다.

Ⅱ. 성과감사 대상 현황

□ 성과감사 점검영역

○ 공사 내부 보안운영규정 및 보안업무절차 등에 대한 적정성 및 효율성을 검토하여 성과감사 대상을 선정하였으며, 그 현황은 다음과 같다.

구분	점검대상	비고
규정	○ 한국국토정보공사정보보안업무지침	
시스템 (운영)	○ 네트워크접근제어(NAC): 비인가 정보시스템 차단 ○ 키보드보안솔루션: 전자우편 보안강화 ○ 다가우저: 불용 전산장비 하드디스크 파기 ○ 유해차단솔류선: 유해싸이트 효과적인 차단정책 적용 ○ 방화벽: 용역업체 업무망과 분리운영 ○ 보안USB: 정보 유출 방지를 위한 보안성 강화 ○ DB 접근제어: 무단 DB접근 통제 ○ 정보자산 보호를 위한 보험	
외부용역 관리	○ 외부영역업체 보안각서 징구 ○ 외부 업체직원 보안 교육 ○ 외부업체 직원의 개발서버 유입 금지 ※ 공간정보사업 및 해외사업 포함	

Ⅲ. 성과감사 결과

1. 「한국국토정보공사정보보안업무지침」에 관한 사항

□ 감사초점

○ 공사 내부규정 중 정보자산과 보안에 위배되는 규정, 규칙, 관행 등을 선제적으로 개선함으로써 보안 취약점 노출을 최소화하고 공사 보안 정책을 최신화하여 정보보안 기반을 확고히 하는 절차 개선 등의 활동이 함께 진행되고 있어야 한다.

○ 이를 위해 내부 규정 개정 및 보안절차 개선 계획을 점검하는 것을 감사초점으로 설정하였다.

□ 판단기준

○ 취약한 정보보안 기준 개선과 최신성 확보로 적절한 정책을 수립하고, 이를 지속적으로 모니터링(평가)하여 당초 목표가 달성되도록 추진되어야 한다.

○ 더불어 보안사고에 따른 사후조치 매뉴얼이 마련되어 적절하게 운영되어야 한다.

○ 이를 판단하기 위하여 다음과 같이 2가지 기준을 설정하였다.

① 「한국국토정보공사정보보안업무지침」은 항상 최신성이 확보되어 있어야 한다. ② 보안사고 발생 시 사후조치를 위한 매뉴얼이 마련되어야 한다.

□ 점검결과

가. 정보보안 사고 발생에 따른 사후관리 절차 강화

○ 최근 개인정보 유출사고가 IT 기술의 발달로 빠른 확산 및 회수가 불가능하며 유출된 정보는 범죄에 악용되는 등 사회적 중대 관심사로 대두되고 있고 우리공사도 측량고객의 개인정보 등을 보관하고 있어 정보보안 사고 발생에 따른 사후조치를 위해 사고 처리기준을 마련해 운영하고 있다.

○ 「정보시스템 도입 보안기준」 제12조(보안사항 위반에 따른 제재조치)에 따르면 “용역업체가 누출금지 정보를 포함하여 정보통신 보호자료 등 공사 내부 자료를 무단으로 유출할 경우 관련법에 따라 민·형사상의 모든 책임을 지며, 용역사업 수행자는 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 별표 1의 ‘누출금지 대상정보’를 준수하여야 하고, 해당 정보 누출 시 「국가계약법 시행령 제76조」에 따라 사업자를 부정당업체로 등록할 수 있도록 하고 있으며, 용역사업자가 한국국토정보공사의 보안정책을 위반하였을 경우 별표 2의 ‘사업자 보안위규 처리기준’에 따라 위규자 및 관리자를 행정 조치하고 별표3의 ‘보안 위약금’을 부과한다.”라고 규정하고 있다.

< 표 1. 사업자 보안위규 처리기준 >

구분	위규사항	처리기준
심각	○ 비밀 및 대외비급 정보 유출 및 유출시도 등	· 사업참여 제한 · 위규자 및 직속 감독자 중징계 · 재발방지를 위한 조치계획 제출 · 위규자 대상 특별 보안교육 실시

중대	○ 비공개 정보 관리 소홀 등	· 위규자 및 직속 감독자 중징계 · 재발방지를 위한 조치계획 제출 · 위규자 대상 특별 보안교육 실시
보통	○ 기관 제공 중요정책·민감 자료 관리소홀 등	· 위규자 및 직속 감독자 경징계 · 위규자 및 직속 감독자 사유서 / 경위서 징구 · 위규자 대상 특별 보안교육 실시
경미	○ 업무 관련서류 관리 소홀 등	· 위규자 서면·구두 경고 등 문책 · 위규자 사유서 / 경위서 징구

※「정보시스템 도입 보안기준」<별표 2> 내용을 가공

○ 이에 따라 용역사업자가 공사의 보안정책을 위반하였을 경우 < 표 1. 사업자 보안위규 처리기준 >에 따라 위규자 및 관리자를 행정조치할 수 있도록 기준을 마련하였다.

< 표 2. 보안 위약금 부과 기준 >

구분	위규 수준			
	A급	B급	C급	D급
위규 사항	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금 규모	부정당업자 등록	사업금액의 5%	사업금액의 3%	사업금액의 2%

※ 위규 수준별로 A ~ D 등급으로 차등 부과

○ 또한 < 표 2. 보안 위약금 부과 기준 >과 같이 보안사고가 발생하는 경우 위규사항에 따라 위약금을 부과할 수 있도록 기준을 마련해 용역사업 발주 시 제안요청서에 명시하고 있다.

○ 그러나 「한국국토정보공사정보보안업무지침」과 「정보시스템 도입 보안기준」에는 보안사고 발생에 따른 후속 업무처리와 위약금 부과 등과 같은 의사결정을 할 수 있는 절차가 마련되어 있지 않다.

○ 결과적으로 보안사고가 발생되는 경우 < 표 1. >과 < 표 2. > 기준에 따라 위규사항을 확인한 후 처리기준에 따라 조치하고 위약금 부과가 필요한 경우 신속히 위약금액을 산정·결정할 수 있도록 업무절차를 마련하는 것이 타당하며, 더불어 동일한 보안사고가 재발되지 않도록 사고처리계획이 수립되는 경우 그 수립된 계획이 적정한지 여부가 심의되고 의결될 수 있도록 업무절차를 구체적으로 마련하는 것이 타당하다.

2. 정보보안시스템 운영에 관한 사항

□ 감사초점

○ 정보시스템을 도입 또는 변경이 발생할 경우, 설계·코딩·테스트·구현 과정에서의 보안대책을 강구하고 보안 관련 적절성을 주기적으로 확인함으로써 보안 취약점을 제거해야 한다.

○ 이에 따라 감사초점은 정보보안 종합대책이 수립되어야 하며, 공사에서 마련한 보안정책이 현업에서 실질적으로 적용되는지 여부 등을 확인함으로써 보안 취약점이 제거되어야 하고, 정보보안 자산들이 적정하게 보호되는 지를 점검하는 것으로 설정하였다.

□ 판단기준

○ 공사에서 운영되는 정보시스템은 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애발생에 대비하여 정보시스템 이원화, 백업관리, 복구 등 종합적인 재난방지 대책을 수립·시행되어야 하며, 이

러한 정보자산은 안전하게 보호되어야 한다. 또한 보안 취약점이 노출되지 않도록 상시적인 점검 등이 수행되어야 한다.

○ 따라서 종합적인 재난방지 대책을 수립·시행되는지와 보안 취약점이 노출되지 않도록 상시적인 점검 등이 적정하게 이루어지고 있는지 판단하기 위하여 다음 4가지 기준을 설정하였다.

① 시스템 관리자는 정보시스템의 변경이 발생할 경우, 정보시스템의 설계·코딩·테스트·구현과정에서의 보안대책을 강구하여야 하며, 보안 관련 적절성을 주기적으로 확인하여야 한다.
② 인위적 또는 자연적인 원인으로 인한 정보통신망의 장애발생에 대비하여 정보시스템 이원화, 백업관리, 복구 등 종합적인 재난방지 대책을 수립·시행되어야 한다
③ 정보보안시스템은 화재보험에 가입되어 있어야 한다. 「재무규정」제45조(부동산 및 회원권의 관리)에 따라 건물, 구축물은 화재보험에 가입할 것
④ 정보유출을 위해 구축된 보안시스템이 적절하게 현업에서 운영되어야 한다.

□ 점검결과

가. 정보보안 취약점 점검을 위한 모의해킹 권고

○ 최근 개인정보 유출사고가 IT 기술의 발달로 빠른 확산 및 회수가 불가능하며 유출된 정보는 범죄에 악용되는 등 사회적 중대 관심사로 대두되고 있고 우리공사도 측량고객의 개인정보 등을 보관하고 있어 국토정보 생성·제공기관으로써의 위상에 걸맞는 최상의 정보보안 체계 구축을 위해 정기적으로 점검을 실시하고 있다.

○ 「한국국토정보공사정보보안업무지침」제27조(서버 보안관리) 제②항에 따르면 “정보보안담당관은 제1항에서 수립한 보안대책의 적절성을 수시 확인하되 연 1회 이상 서버 설정 정보 및 저장자료의 절취, 위·변조 가능성 등 보안취약점을 점검하여야 한다.”라고 규정하

고 있으며, 「같은 지침」제33조(네트워크장비 보안관리)에 따르면 “펌웨어 무결성 및 소프트웨어·서버 운영체제 취약점과 최신 업데이트 여부를 주기적으로 확인하여 항상 최신 버전으로 유지”하도록 규정하고 있다.

< 최근 취약점 개선 현황 >

○ △△△△부 점검결과에 따른 정보시스템 및 웹사이트 취약점 보완 조치 결과 제출(2014.12.29.) ※ 네트워크 취약점 등 개선

○ △△△△부 점검결과에 따른 정보시스템 및 웹사이트 취약점 보완 조치 결과 제출(2015.4.24.) ※ 서버취약점 등 개선

○ 그러나 정보시스템 및 네트워크 취약점 점검이 도입시점에 대부분 이루어지고 있어 정보시스템 환경변화에 따른 네트워크 및 기능 변경과 사용자 편의를 위해서 개선된 업무프로세스 개선 등에 따라 변경된 코딩 등에 대한 정기적인 취약점 점검이 내부 유지보수 업체에 의해서 자율적으로 이루어지고 있는 실정이다.

○ 결과적으로 정보시스템 및 네트워크 등에 대한 외부 지적사항이 지속적으로 발생하고 있으며, 그 조치결과에 대해 외부 기준에 따라 확인 하는 절차가 미흡한 것으로 보여지고 있어 보안사고 예방과 취약점 개선을 위해 모의해킹 등과 같은 보안정책 도입을 통해 정보보안 정책의 실효성을 확보하는 것이 타당하다.

나. 정보자산 보호를 위한 화재보험 가입 방법 개선

○ 공사에서는 2000년 이후 업무의 효율성 향상을 위하여 공사의 지적측량과 공간정보 사업 그리고 재무회계 업무와 같은 대부분의 업무를 IT 기반의 정보시스템으로 전환해 운영하고 있으며, 현재 △△△

△처에서 구입 및 운영하고 있는 주요 전산자산으로는 통합서버 등 총 2,747대 65억 8492만 원(취득가액)이다.

○ 「부동산관리규칙」제20조(보험의 가입) 제①항에 따르면 “관리책임자는 토지를 제외한 유형자산은 화재보험에 가입하여야 한다.”라고 규정되어 있으며, 제②항에 따르면 “보험금액은 장부가액을 기준으로 하되 장부가액이 현저히 낮을 경우에는 현재가액(시가액)으로 하며 보험기간은 1년으로 한다.”라고 규정하고 있다.

< 본사 화재보험가입 현황 >

○ 전산장비 화재보험 갱신(₩₩₩₩처-5336, 2014.12.24.)

- 보험기간: 2014.12.24. ~ 2015.12.24.
- 보험금액: 11,567,841,054원(2014년도 전산장비 미상각잔액)

※ 수량: 10,224대 / 취득가액: 41,479,770,264원

※ 본사 건물화재보험과 중복되어 건물실화보험 제외

- 보 험 료: 1,307,100원

< 표 4. 2014년도 보험가입 대상 주요 장비 현황 >

구분	품명	수량	미상각잔액	비고
계		16	5,441,959,001	
하드웨어	바로처리센터 서버 등	2	297,464,792	
소프트웨어	**대국민 모바일 앱 등**	**14**	**5,144,494,209**	

※ 미상각잔액 1억원 이상 전산장비만 산출

○ 그러나 관련규정에 따라 유형자산[1]은 화재보험에 가입하도록 되어

있음에도 < 표 4 >와 같이 라이선스로 자산의 관리가 가능한 O/A 소프트웨어, 개발 소프트웨어 등이 화재보험에 가입되어 있는 것을 확인할 수 있어 보험대상장비 선정을 재획정하는 것이 타당한 것으로 나타났다.

○ 또한 2014. 12. 24.이후 구입되어 △△△△처 전산실에서 사용되고 있는 주요 전산장비(스토리지/서버 등)가 화재보험에 미가입되어 있는 등 재난발생에 따라 예방적으로 가입하고 있는 화재보험 갱신에 최신성이 떨어지고 있다.

○ 결과적으로 본사 △△△△처에서 운영하는 주요 전산자원에 대한 보험가입 대상 장비를 정확히 식별하고 가입 이후 신규 구입·폐기 등의 변화가 발생하는 경우 즉시 반영함으로써 사고발생 시 충분한 보상이 가능하도록 화재보험을 관리하는 것이 타당하다.

다. 정보 유출 차단을 위한 USB 차단 정책 강화

○ 공사에서는 정보시스템 보안취약점 점검의 실효성 제고와 최근 증가하고 있는 메일과 USB를 통한 악성코드 유입 및 중요자료 유출 사고에 적극 대비하고자 “정보시스템 USB 포트 잠금장치”[2]를 도입 운영하고 있다.

○ △△△△부 “정보시스템 USB 포트 보안 강화 등 요청[3]”에 따르면

---

1) 유형자산: 경영수단으로 반복사용되며 구체적인 형태를 갖춘 고정자산으로 유형자산은 기업의 영업목적을 달성하기 위하여 장기간에 걸쳐 계속 사용할 목적으로 보유하고 있는 자산이다. 유형자산의 종류로는 ① 토지 ② 건물 ③ 기계장치 ④ 구축물 ⑤ 선박 ⑥ 차량운반구 ⑦ 공구와 기구 ⑧ 비품 ⑨ 건설중인 자산 등이 있다.

2) 정보시스템 USB 포트 보안 강화 조치결과 제출(WWWW처-1151, 2015.3.24.)

3) 정보시스템 USB 포트 보안 강화 등 요청(WWWW부 WWWWWW관-1155, 2015.2.27.)

공사에서 운영하는 정보시스템과 단말기의 USB 포트에 대해 봉인을 실시하고, 부득이 USB를 사용하는 경우 정보보안담당관 승인하에 등록된 USB만 사용하고 관리대장에 기록유지 하도록 하였다.

○ 이에 따라 △△△△처에서 설치한 “정보시스템 USB 포트 잠금장치” 운영 현황을 점검한 결과 전산실 등에 설치된 서버에 “정보시스템 USB 포트 잠금장치”가 설치된 것을 확인 할 수 있는 반면 공사 정보화사업 관련 사업에 참여하고 있는 용역업체들을 대상으로 공사의 보안정책 안내와 용역사업 참여 직원을 대상으로 하는 보안교육 시 “정보시스템 USB 포트 잠금장치”에 대한 보안내용을 반영해 교육을 실시하도록 요청하는 등의 체계적인 관리가 필요한 것으로 보여지고 있다.

○ 더불어 공사에서 “정보시스템 USB 포트 잠금장치” 도입 시점이 2015. 3월인 것을 감안하면 일정기간 동안은 “정보시스템 USB 포트 잠금장치”에 대한 점검을 상시적으로 실시함으로써 그 실효성을 확보할 필요가 있다.(△△△△부에서는 “정보시스템 USB 포트 잠금장치”에 대해서 분기별로 봉인상태를 점검하도록 권고하고 있음.)

○ 결국 “정보시스템 USB 포트 잠금장치” 설치 후 USB 포트 봉인상태를 정기적으로 점검하고 유지보수 업체직원 교육 시 그 내용을 교육할 수 있도록 보안관리체계를 강화하는 것이 타당하다.

3. 외부 용역업체 관리에 관한 사항

□ 감사초점

○ 공사의 정보화·정보보호사업 및 보안컨설팅 수행 등을 외부용역으로 추진할 경우 사업 책임자로 하여금 용역사업 수행 관련 보안교육·점검 및 용역기간 중 참여인력 임의교체 금지 등이 포함된 보안대책을 수립·시행하도록 하여야 하며, 외부 용역사업에 따라 생성되어지고 있는 성과물 관리에 취약점은 없는 지를 점검하는 것으로 감사초점을 설정하였다.

□ 판단기준

○ 외부 용역을 위해 공사에 상주하는 인력에 대해 적정한 보안교육이 이루어지고 있는지 여부와 외부 용역사업에 따라 생성되는 성과물이 적정한 보안정책과 시스템에서 보호되고 있는지 여부를 판단하기 위해 다음과 같이 기준을 설정하였다.

① 외부 영역사업으로 추진되어 생성되는 성과물을 위한 공사 보안관리정책이 마련되어야 한다.(공사내부가 아닌 외부 용역업체에서 상주 사업을 하는 경우)

□ 점검결과

가. 외부용역사업에 따라 생성·제공되는 정보의 보안관리체계 강화 권고

○ 공사에서는 2015년도 정보화 전략사업(BPR/ISP) 및 공간정보 DB 구축 사업, 러시아 사할린 한인묘지 현황 파악 해외사업 등 다양한 용역사업을 추진하고 있다.

○ 「보안업무지침」제52조(용역업체에 대한 보안대책) 제①항에 따르면

“외부용역을 발주할 때에는 용역회사 대표자 및 참여자에 대한 보안대책, 용역사업 참여자 외 접근방지대책, 용역관련 각종자료의 보안관리 대책, 용역성과물, 유인물의 보안관리 대책 등의 사항을 고려하여 보안대책을 수립, 당해 소속 분임보안담당관(대외비용역은 보안담당관)에게 그 적정성 여부에 대하여 보안성 검토를 서면으로 받은 후 이를 과업지시서에 명시하여야 한다.”라고 규정하고 있다.

< 용역사업 과업지시서 보안 내용(일반) >

1. 계약업체는 사업수행에 사용되는 인원, 문서, 장비 등의 보안관리 계획을 수립하여야 하며, 보안상 결격사항이 없도록 조치하여야 한다.
2. 계약업체는 사업 수행과정에서 취득한 자료와 정보에 관해서는 사업수행의 전후를 막론하고 공사의 승인 없이 외부에 유출 또는 누설하여서는 아니 된다.
3. 보안사항 위반에 따른 제재조치
4. 계약업체는 사업 수행 중 인원, 문서 및 전산자료 보안 등 아래의 보안관리 사항을 준수하여야 한다. 기타 사항은 공사「보안업무지침」에서 정하는 바에 따른다.
   가. 참여 인력에 대한 보안관리
   나. 문서 및 전산자료보안
   다. 사무실 및 매체·장비 반출입 보안
   라. 네트워크 접근 보안
5. 보안사항 위반에 따른 제재조치

※ △△△△△△실 2014년도 국토조사용 시스템 개발 제안요청서를 가공함

○ 이에 따라 공간정보 관련 시스템을 개발 및 구축하는 경우 용역사업 과업지시서에 “용역사업 보안관리 방안”을 명시하고 사업수행자에게 반드시 준수하도록 하고 있으나, 발주부서의 실질적인 준수여부 점검 없이 단순히 사업수행자의 자율적인 준수를 기대하는 수준에 머물러 있는 실정이며, 결국 업체·참여자의 보안각서 등을 징구하거나 자율적인 교육 등을 실시하는 오프라인 보안관리 방안에 의

존하고 있는 것으로 나타나고 있다.

○ 즉 외부에서 이루어지는 용역사업의 경우 공사에서 제공한 정보를 적정하게 통제할 수 있는 방법이 없어 외부용역업체가 불적정한 방법으로 공사에서 제공한 정보를 보관 또는 타 기관에 제공하는 경우 보안에 취한 것으로 보여지고 있다. 따라서 사전적 정보 유출사고 예방 등을 위해 보다 강화된 보안체계 운영이 요구되고 있다.

○ 결과적으로 근본적인 유출을 사전에 차단할 수 있는 네트워크 차단 방안을 확대함으로써 공간과 용역 수행 직원(권한) 임의 변경 등에 따른 취약점을 사전에 차단할 수 있도록 보안관리 체계를 강화할 필요가 있는 것으로 보여진다.

Ⅳ. 지적사항에 대한 처분요구

□ 붙　임: 감사결과 처분요구서 5부.　끝.

한국국토정보공사 상임감사

개 선

제 목 정보보안 사고 발생에 따른 사후관리 절차 강화

관 계 기 관 △△△△처

내 용

한국국토정보공사(△△△△처)는 최근 개인정보 유출사고가 IT 기술의 발달로 빠른 확산 및 회수가 불가능하며 유출된 정보는 범죄에 악용되는 등 사회적 중대 관심사로 대두되고 있어 정보보안 사고 발생에 따른 사후 조치를 위해 사고 처리기준을 마련해 운영하고 있다.

위 공사「정보시스템 도입 보안기준」제12조(보안사항 위반에 따른 제재조치)에 따르면 “용역업체가 누출금지 정보를 포함하여 정보통신 보호자료 등 공사 내부 자료를 무단으로 유출할 경우 관련법에 따라 민·형사상의 모든 책임을 지며, 용역사업 수행자는 사업 수행에 사용되는 문서, 인원, 장비 등에 대하여 물리적, 관리적, 기술적 보안대책 및 별표 1의 ‘누출금지 대상정보’를 준수하여야 하고, 해당 정보 누출 시 「국가계약법 시행령 제76조」에 따라 사업자를 부정당업체로 등록할 수 있도록 하고 있으며, 용역사업자가 한국국토정보공사의 보안정책을 위반하였을 경우 별표 2의 ‘사업자 보안위규 처리기준’에 따라 위규자 및 관리자를 행정 조치하고 별표3의 ‘보안 위약금’을 부과한다.”라고 규정하고 있다.

[표 1] 사업자 보안위규 처리기준

구분	위규사항	처리기준
심각	○ 비밀 및 대외비급 정보 유출 및 유출시도 등	· 사업참여 제한 · 위규자 및 직속 감독자 중징계 · 재발방지를 위한 조치계획 제출 · 위규자 대상 특별 보안교육 실시
중대	○ 비공개 정보 관리 소홀 등	· 위규자 및 직속 감독자 중징계 · 재발방지를 위한 조치계획 제출 · 위규자 대상 특별 보안교육 실시
보통	○ 기관 제공 중요정책·민감 자료 관리소홀 등	· 위규자 및 직속 감독자 경징계 · 위규자 및 직속 감독자 사유서 / 경위서 징구 · 위규자 대상 특별 보안교육 실시
경미	○ 업무 관련서류 관리 소홀 등	· 위규자 서면·구두 경고 등 문책 · 위규자 사유서 / 경위서 징구

※「정보시스템 도입 보안기준」<별표 2> 내용을 가공

이에 따라 용역사업자가 공사의 보안정책을 위반하였을 경우 [표 1]사업자 보안위규 처리기준에 따라 위규자 및 관리자를 행정 조치할 수 있도록 기준을 마련하였다.

[표 2] 보안 위약금 부과 기준

구분	위규 수준			
	A급	B급	C급	D급
위규 사항	심각 1건	중대 1건	보통 2건 이상	경미 3건 이상
위약금 규모	부정당업자 등록	사업금액의 5%	사업금액의 3%	사업금액의 2%

※ 위규 수준별로 A ~ D 등급으로 차등 부과

또한 [표 2]보안 위약금 부과 기준과 같이 보안사고가 발생하는 경우 위규사항에 따라 위약금을 부과할 수 있도록 기준을 마련해 용역사업 발주시 제안요청서에 명시하고 있다.

그러나 위 공사 「한국국토정보공사정보보안업무지침」과 「정보시스템 도입 보안기준」에는 보안사고 발생에 따른 후속 업무처리와 위약금 부과 등과 같은 의사결정을 할 수 있는 절차가 마련되어 있지 않다.

결과적으로 보안사고가 발생되는 경우 [표 1]과 [표 2] 기준에 따라 위규사항을 확인한 후 처리기준에 따라 조치하고 위약금 부과가 필요한 경우 신속히 위약금액을 산정·결정할 수 있도록 업무절차를 마련하는 것이 타당하며, 더불어 동일한 보안사고가 재발되지 않도록 사고처리계획이 수립되는 경우 그 수립된 계획이 적정한지 여부가 심의되고 의결될 수 있도록 업무절차를 구체적으로 마련하는 것이 타당하다.

조치하여야 할 사항

한국국토정보공사(△△△△처장)은 정보보안 사고 발생 시 「정보시스템 도입 보안기준」에 따라 사후조치(관리)가 신속하게 이루어 질 수 있도록 업무처리절차(보안사고처리 매뉴얼 등)를 구체적으로 마련하시기 바랍니다.

한국국토정보공사 상임감사

권 고

제 목 정보보안 취약점 점검을 위한 모의해킹 실시

관 계 기 관 △△△△처

내 용

최근 개인정보 유출사고가 IT 기술의 발달로 빠른 확산 및 회수가 불가능하며 유출된 정보는 범죄에 악용되는 등 사회적 증대 관심사로 대두되고 있고 우리공사도 측량고객의 개인정보 등을 보관하고 있어 국토정보 생성·제공기관으로써의 위상에 걸맞는 최상의 정보보안 체계 구축을 위해 정기적으로 점검을 실시하고 있다.

「한국국토정보공사정보보안업무지침」제27조(서버 보안관리) 제②항에 따르면 “정보보안담당관은 제1항에서 수립한 보안대책의 적절성을 수시 확인하되 연 1회 이상 서버 설정 정보 및 저장자료의 절취, 위·변조 가능성 등 보안취약점을 점검하여야 한다.”라고 규정하고 있으며, 「같은 지침」 제33조(네트워크장비 보안관리)에 따르면 “ 펌웨어 무결성 및 소프트웨어·서버 운영체제 취약점과 최신 업데이트 여부를 주기적으로 확인하여 항상 최신 버전으로 유지”하도록 규정하고 있다.

< 최근 취약점 개선 현황 >

○ △△△△부 점검결과에 따른 정보시스템 및 웹사이트 취약점 보완 조치 결과 제출 (2014.12.29.) ※ 네트워크 취약점 등 개선

○ △△△△부 점검결과에 따른 정보시스템 및 웹사이트 취약점 보완 조치 결과 제출 (2015.4.24.) ※ 서버취약점 등 개선

그러나 정보시스템 및 네트워크 취약점 점검이 도입시점에 대부분 이루어지고 있어 정보시스템 환경변화에 따른 네트워크 및 기능 변경과 사용자 편의를 위해서 개선된 업무프로세스 개선 등에 따라 변경된 코딩 등에 대한 정기적인 취약점 점검이 내부 유지보수 업체에 의해서 자율적으로 이루어지고 있는 실정이다.

결과적으로 정보시스템 및 네트워크 등에 대한 외부지적사항이 지속적으로 발생하고 있으며, 그 조치결과에 대해 외부 기준에 따라 확인 하는 절차가 미흡한 것으로 보여지고 있어 보안사고 예방과 취약점 개선을 위해 모의해킹 등과 같은 보안정책 도입을 통해 정보보안 정책의 실효성을 확보하는 것이 타당하다.

조치하여야 할 사항

한국국토정보공사(△△△△처장)은 내부적으로 고위험 영역으로 분류되고 있는 취약점에 대해서는 모의해킹 등과 같은 보안정책 도입을 통해 정보보안정책의 실효성 확보와 보안사고 예방체계 강화를 권고합니다.

한국국토정보공사 상임감사

시 정

제 목 정보자산 보호를 위한 화재보험 가입 방법 개선

관 계 기 관 △△△△처

내 용

공사에서는 2000년 이후 업무의 효율성 향상을 위하여 공사의 지적측량과 공간정보 사업 그리고 재무회계 업무와 같은 대부분의 업무를 IT 기반의 정보시스템으로 전환해 운영하고 있으며, 현재 △△△△처에서 구입 및 운영하고 있는 주요 전산자산으로는 통합서버 등 총 2,747대 65억 8492만원(취득가액)이다.

「부동산관리규칙」제20조(보험의 가입) 제①항에 따르면 “관리책임자는 토지를 제외한 유형자산[4]은 화재보험에 가입하여야 한다.”라고 규정되어 있으며, 제②항에 따르면 “보험금액은 장부가액을 기준으로 하되 장부가액이 현저히 낮을 경우에는 현재가액(시가액)으로 하며 보험기간은 1년으로 한다.”라고 규정하고 있다.

따라서 공사에서 보관하고 있는 모든 유형자산은 재산상 손해를 방지하기 위해 화재보험에 가입하여 자산을 보호하기 위한 방안을 강구해야 한다.

---

4) 유형자산: 경영수단으로 반복사용되며 구체적인 형태를 갖춘 고정자산으로 유형자산은 기업의 영업목적을 달성하기 위하여 장기간에 걸쳐 계속 사용할 목적으로 보유하고 있는 자산이다. 유형자산의 종류로는 ① 토지 ② 건물 ③ 기계장치 ④ 구축물 ⑤ 선박 ⑥ 차량운반구 ⑦ 공구와 기구 ⑧ 비품 ⑨ 건설중인 자산 등이 있다.

< 본사 화재보험가입 현황 >

○ 전산장비 화재보험 갱신(₩₩₩₩처-5336, 2014.12.24.)

- 보험기간: 2014.12.24. ~ 2015.12.24.
- 보험금액: 11,567,841,054원(2014년도 전산장비 미상각잔액)

※ 수량: 10,224대 / 취득가액: 41,479,770,264원

※ 본사 건물화재보험과 중복되어 건물실화보험 제외

- 보 험 료: 1,307,100원

이에 따라 △△△△처는 2014. 12. 24. 시점에 관리되고 있는 유형자산과 무형자산을 대상으로 화재보험을 가입하였으나 보험가입 이후 취득한 정보자산 744대 3,171,207,265원(유형자산과 무형자산 전체)은 미가입되어 있는 등 재난발생에 따라 예방적으로 가입하고 있는 화제보험 갱신에 최신성이 떨어지고 있다.

[표 3] 2014년도 보험가입 대상 주요 장비 현황

구분	품명	수량	미상각잔액(원)	비고
계		16	5,441,959,001	
하드웨어	바로처리센터 서버 등	2	297,464,792	
소프트웨어	**대국민 모바일 앱 등**	**14**	**5,144,494,209**	

※ 미상각잔액 1억원 이상 전산장비만 산출하였음.

또한 [표 3]2014년도 보험가입 대상 주요 장비 현황과 같이 별도의 보험 없이 라이선스로 자산관리가 가능한 S/W 등 무형자산 5,144,494,209원이 화재보험에 가입되어 있다.

결과적으로 본사 △△△△처에서 운영하는 주요 전산자원에 대한 보험 가입 대상장비를 정확히 식별하고 가입 이후 신규 구입·폐기 등의 변화가 발생하는 경우 즉시 반영함으로써 사고발생 시 충분한 보상이 가능하도록 화재보험 방법을 개선하는 것이 타당하다.

조치하여야 할 사항

한국국토정보공사(△△△△처장)은 전산자원 보호를 위해 가입되어 있는 2014년도 화재보험 가입금액 중 5,144,494,209원에 대해서는 추후 가입 시 제외(취소)하시기 바라며, 보험가입 이후 신규 구입·폐기 등의 변화가 발생하는 경우 즉시 반영할 수 있도록 가입방법을 개선하시기 바랍니다.

한국국토정보공사 상임감사

개 선

제 목 정보 유출 차단을 위한 USB 차단 정책 강화

관 계 기 관 △△△△처

내 용

공사에서는 정보시스템 보안취약점 점검의 실효성 제고와 최근 증가하고 있는 메일과 USB를 통한 악성코드 유입 및 중요자료 유출 사고에 적극 대비하고자 “정보시스템 USB 포트 잠금장치”[5]를 도입 운영하고 있다.

△△△△부 “정보시스템 USB 포트 보안 강화 등 요청[6]”에 따르면 공사에서 운영하는 정보시스템과 단말기의 USB 포트에 대해 봉인을 실시하고, 부득이 USB를 사용하는 경우 정보보안담당관 승인하에 등록된 USB만 사용하고 관리대장에 기록·유지하도록 하였다.

이에 따라 △△△△처에서 설치한 “정보시스템 USB 포트 잠금장치” 운영 현황을 점검한 결과 전산실 등에 설치된 서버에 “정보시스템 USB 포트 잠금장치”가 설치된 것을 확인 할 수 있는 반면 공사 정보화사업 관련 사업에 참여하고 있는 용역업체들을 대상으로 공사의 보안정책 안내와 용역사업 참여 직원을 대상으로 하는 보안교육 시 “정보시스템 USB 포트

---

5) 정보시스템 USB 포트 보안 강화 조치결과 제출(WWWW처-1151, 2015.3.24.)

6) 정보시스템 USB 포트 보안 강화 등 요청(WWWW부 WWWWWW관-1155, 2015.2.27.)
   가. 운영중인 정보시스템과 단말기의 USB 포트 봉인
   나. 부득이 하게 USB 사용 시 정보보안담당관 승인 하에 등록된 USB만 사용하고 관리대장에 기록 유지
   다. 분기별로 확인하고 기록

잠금장치”에 대한 보안내용을 반영해 교육을 실시하도록 요청하는 등의 체계적인 관리가 필요한 것으로 보여지고 있다.

더불어 공사에서 “정보시스템 USB 포트 잠금장치” 도입 시점이 2015. 3월인 것을 감안하면 일정기간 동안은 “정보시스템 USB 포트 잠금장치”에 대한 점검을 상시적으로 실시함으로써 그 실효성을 확보할 필요가 있는 것으로 나타나고 있다.(△△△△부에서는 “정보시스템 USB 포트 잠금장치”에 대해서 분기별로 봉인상태를 점검하도록 권고하고 있음.)

결국 “정보시스템 USB 포트 잠금장치” 설치 이후 그 봉인상태를 정기적으로 점검하고 유지보수업체직원 교육 시 그 내용을 교육할 수 있도록 보안관리체계를 강화하는 것이 타당하다.

조치하여야 할 사항

한국국토정보공사(△△△△처장)은 “정보시스템 USB 포트 잠금장치” 보안정책이 안정적으로 정착될 수 있도록 「정보시스템 도입 보안기준」 등에 점검프로세스를 마련하시기 바라며, 유지보수업체직원 교육 시 “정보시스템 USB 포트 잠금장치” 보안정책이 교육될 수 있도록 관련업체에 공사 정책을 안내하여 주시기 바랍니다.

한국국토정보공사 상임감사

권 고

제 목 외부용역사업에 따라 생성·제공되는 정보의 보안관리체계 강화

관 계 기 관 △△△△처

협 조 기 관 △△△△△△실, △△△△△처

내 용

공사에서는 2015년도 정보화 전략사업(BPR/ISP) 및 공간정보 DB 구축 사업, 러시아 사할린 한인묘 현황 파악 해외사업 등 다양한 용역사업을 추진하고 있다.

「보안업무지침」제52조(용역업체에 대한 보안대책) 제①항에 따르면 “외부용역을 발주할 때에는 용역회사 대표자 및 참여자에 대한 보안대책, 용역사업 참여자 외 접근방지대책, 용역관련 각종자료의 보안관리 대책, 용역성과물, 유인물의 보안관리 대책 등의 사항을 고려하여 보안대책을 수립, 당해 소속 분임보안담당관(대외비용역은 보안담당관)에게 그 적정성 여부에 대하여 보안성 검토를 서면으로 받은 후 이를 과업지시서에 명시하여야 한다.”라고 규정하고 있다.

< 용역사업 과업지시서 보안 내용(일반) >

1. 계약업체는 사업수행에 사용되는 인원, 문서, 장비 등의 보안관리 계획을 수립하여야 하며, 보안상 결격사항이 없도록 조치하여야 한다.
2. 계약업체는 사업 수행과정에서 취득한 자료와 정보에 관해서는 사업수행의 전후를 막론하고 공사의 승인 없이 외부에 유출 또는 누설하여서는 아니 된다.

3. 보안사항 위반에 따른 제재조치
4. 계약업체는 사업 수행 중 인원, 문서 및 전산자료 보안 등 아래의 보안관리 사항을 준수하여야 한다. 기타 사항은 공사「보안업무지침」에서 정하는 바에 따른다.
  가. 참여 인력에 대한 보안관리
  나. 문서 및 전산자료보안
  다. 사무실 및 매체·장비 반출입 보안
  라. 네트워크 접근 보안
5. 보안사항 위반에 따른 제재조치

※ △△△△△△실 2014년도 국토조사용 시스템 개발 제안요청서를 가공함

이에 따라 공간정보 관련 시스템을 개발 및 구축하는 경우 용역사업 과업지시서에 “용역사업 보안관리 방안”을 명시하고 사업수행자에게 반드시 준수하도록 하고 있으나, 발주부서의 실질적인 준수여부 점검 없이 단순히 사업수행자의 자율적인 준수를 기대하는 수준에 머물러 있는 실정이며, 결국 업체·참여자의 보안각서 등을 징구하거나 자율적인 교육 등을 실시하는 오프라인 보안관리 방안에 의존하고 있는 것으로 나타나고 있다.

즉 외부에서 이루어지는 용역사업의 경우 공사에서 제공한 정보를 적정하게 통제할 수 있는 방법이 없어 외부용역업체가 불적정한 방법으로 공사에서 제공한 정보를 보관 또는 타 기관에 제공하는 경우 보안에 취한 것으로 보여지고 있다. 따라서 사전적 정보 유출사고 예방 등을 위해 보다 강화된 보안체계 운영이 요구되고 있다.

결과적으로 근본적인 유출을 사전에 차단할 수 있는 네트워크 차단방안을 확대함으로써 공간과 용역 수행 직원(권한) 임의 변경 등에 따른 취약점을 사전에 차단할 수 있도록 보안관리 체계를 강화할 필요가 있는 것으로 보여진다.

조치하여야 할 사항

한국국토정보공사(△△△△처장)은 공사에서 발주하는 다양한 용역사업이 사업수행자의 업무위치 및 참여직원 변경 등에 따라 발생될 수 있는 정보보안 취약점을 사전에 차단될 수 있도록 네트워크 차단 방안 등과 같은 보안정책을 강화하시기 바랍니다.