□특집□

CALS와 보안관리

신 동 익†

◈ 목 차 ◈

1. 서 론

최근 우리나라는 정보화 사회의 진입을 위하여 막대한 투자와 노력을 기울이고 있다. 이중에서 특히 많은 관심이 집중되고 있는 분야는 산업정보화로서, 우리나라 산업의 정보화를 통하여 산업경쟁력을 향상시키자는 것에 촛점을 맞추고 있다. 산업정보화는 CALS로 흔히 지칭되고 있으며, 이는 CALS가 미 국방부의 무기체계 획득 및 군수지원(Computer-Aided Acquisition and Logistic Support)의 개념에서 일반화, 광범위화되어 민수분야에 확대 적용되면서 구매 및 생명주기상에서의 지속적 지원(Continuous Acquisition and Life-Cycle Support)으로 인식되고, 최근에는 EDI와의 통합을 통하여 초고속 전자거래 환경(Commerce At Light Speed)으로까지 확대되어 발전되므로서 일반적인 지칭이 되었다[1].

일반적으로 정보화는 많은 순기능들 즉 편리함이나 신속함 등의 좋은 측면을 위하여 추진되나, 반면에 많은 역기능들을 동반할 수 있다. 대표적인 사례는 해커들의 침투로 인한 정보의 파괴/누설, 바이러스 감염으로 인한 정보자원의 손상 등을 들수 있다. 이와같은 역기능을 방지하는 것이 정보화시대에서는 중요한 이슈이며 이러한 문제를 해결하기 위하여 많은 연구자와 실무자들이 정보기술 보안에 관하여 연구 및 대책수립에 골몰하고 있다. CALS 역시 다른 정보기술과 마찬가지로 유사한 위협에 노출되어 있으며 이러한 위협을 극복하기 위해서는 적절한 보안대책의 수립과 관리가 필요하다. 본 논문은 보안대책 자체의 기술적 측면보다는 관리적 측면에서의 이슈들을 중점적으로 다루고자 한다. 보안대책에 대하여는 많은 연구와 제품개발들이 수행되고 있으나 상대적으로 보안관리에 대하여는 중요성이 작게 부과되어 있고, 이는 실제로 보안 측면에서 커다란 위협이 될 수 있기 때문이다[2, 3].

2. 보안의 주요 원칙

보안 하면 우리는 흔히 보안소프트웨어나 암호화장비와 같은 보안제품을 연상한다. 그러나 실제로 보안에서 가장 중요한 점은 이와같은 제품 수준에서의 보안이 아니라 좀더 상위수준에서 먼저

† 정회원 한국전산원 책임연구원

보안을 고려해야 한다는 것이다. 영국에서는 정부기관의 IT 보안을 위해 CCTA(Central Computer and Telecommunication Agency)의 Security and Infrastructure Group에서 지침을 제공하고 있다. 지침중 특히 "IT 보안의 감독을 위한 지침"은 매우 유용한 기본적인 원칙들을 제시하고 있다[4]. 여기서는 위 지침에서 제시된 원칙중에서 세가지만 소개한다.

(1) 보안은 조직의 성공을 위해 필수적이다.

조직은 조직 목표의 성공적 달성을 위해서는 정보를 사용한다. 정보는 조직내에서 물리적 장비나 인적자원과 마찬가지로 주요한 자원이다. 따라서 정보와 정보를 처리하는 IT 시스템은 적절한 보호를 필요로 한다. 최근 Hacking과 Virus 등에 의한 정보의 불법적 누설과 수정, 파괴는 조직의 사업에 심각한 영향을 초래할 수 있다. 이외에도 화재와 같은 경우도 정보 이용을 불가능하게 하므로서 조직 사업 추진에 막대한 영향을 끼칠수 있다. 따라서 IT 보안은 조직의 성공을 위해서는 필수적으로 갖추어야 할 요건이다.

(2) 보안은 경영의 문제이지 기술의 문제가 아니다.

IT 보안하면 흔히 보안소프트웨어나 암호를 먼저 연상하기 쉽다 또한 보안사고하면 Virus나 Hacking과 같은 것만 먼저 생각하기 쉽다. 그러나 영국에서 1990년 조사한 결과에 의하면 41%가 사기에 의한 것이고 나머지가 Virus나 Hacking에 의한 것으로 보고되고 있다. 이는 보안이 단순히 기술의 문제가 아님을 보여주고 있다. 기본적으로 보안은 IT 시스템과 정보에 대한 막대한 투자를 보호하고, IT 시스템에 대한 의존성을 정당화 하기 위한 것으로 생각해야 한다 따라서 IT 보안은 경영적 이슈이며, 경영적 차원에서 부터 고려되어야 한다.

(3) 위험은 실재이며 무시될 수 없다.

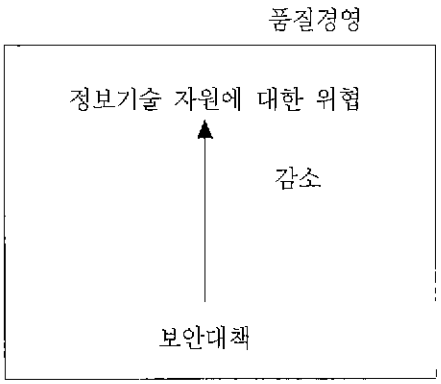
많은 보고서는 IT 시스템에 대한 위협요인을 열거하고 있으며, 이러한 위협을 무시하고 대책을 세우지 않을 경우 초래되는 바람직하지 않은 결과에 대해 경고하고 있다. IT 시스템에 대한 위협은 다양하며. 이들을 단순히 무시할때 생기는 위험은 조직에 심각한 영향을 초래할 수 있다. IT 보안을 위해서는 조직의 IT 시스템에 대한 위협을 식별하고, IT 자산의 취약성을 파악하여, IT 시스템의 위험도를 측정하는 작업이 선행되어야 한다. 이를 기초로 적절한 위험 수준까지 위험도를 낮추기 위해 보안대책을 선정하며, 보안대책의 선정시는 비용효과분석을 통한 합리적 선택이 이루어져야 한다.

위에서 제시된 주요 원칙들을 볼때 보안이 단순히 보안제품을 선정하여 시스템에 구현하는 것에 국한되는 것이 아니고, 좀더 상위수준 즉 경영차원에서 다루어야 할 이슈임을 알 수 있다. 보안은 이제 단순히 보안담당자나 전산담당자가 덤으로 수행하는 부가적인 임무가 아니고 최고경영층이 관심을 갖고 관리적 차원에서 다루어야 할 이슈이다. 따라서 보안의 관리적 측면에서의 대책수립과 구현은 보안 서비스나 메카니즘들을 구현한 보안제품의 선정과 적용이전에 먼저 고려되어야 할 중요한 이슈이며, 이를 체계적으로 수행하기 위한 골격의 수립과 적용이 중요하다. 본 논문은 이러한 점에서 보안관리의 중요성을 강조하고 관리체계의 수립을 위한 기본분석을 제공하고자 한다.

3. 품질경영체계와 보안관리

품질경영이라는 말은 최근 ISO9000의 활발한 적용으로 인하여 많이 알려졌으며, 우리나라의 많은 기업들도 ISO9000 인증을 받기 위하여 노력하고 있다[5]. ISO9000 표준은 산업의 경쟁력 향상을 위해서는 품질의 향상이 필수적이라고 보고, 품질 향상을 위한 기본체계를 제시하고 있다. ISO8402는 품질을 고객의 명시적 혹은 묵시적 요

구사항을 충족시킬 능력을 지니는 제품 특성의 전체라고 정의하고 있다[6]. 다시 말하면 품질이란 목적적합성(fit for purpose)이라고 정의하고 있다. 따라서 품질의 의미는 다양한 분야에 적용될 수 있으며, 보안 측면에서도 적용될 수 있다. 보안이란 정보기술 자원에 대한 위협을 감소시키기 위해서 보안대책을 설정하는 것으로, 이와같은 과정이 품질경영체계의 도움을 받을 경우 더욱 향상된 효과를 낼 수 있다.



(그림 1) 보안과 품질경영

정보기술 자원에 대한 위협에는 여러가지 종류가 있겠으나, 흔히 위협은 의도적인 것과 우발적인 것으로 분류된다. 의도적 위협은 고의로 특정 목적을 위해 자원을 손상, 파괴, 노출시키는 것을 의미하며, 해커에 의한 정보의 손상과 같은 것이 예가 될 수 있다. 반면에 우발적인 위협은 실수나 인식의 부족 등으로 인하여 정보자원에 손상이 생기는 경우를 말하며, 이러한 위협은 관심과 노력이 기울여지면 크게 줄일수 있다. 품질은 품질과 관련된 절차나 책임을 잘 정립하여 무결함 개발상태를 유지하는 것이며, 이러한 개념이 보안 노력에 접목될 경우 보안 위협을 줄이는데 크게 공헌할 수 있다. 따라서 보안은 품질과 같이 경영적 측면에서 먼저 접근하는 것이 필요하며, 최고경영층으로 부터 방향과 의지의 부족은 보안대책의 일관성 부족과 부적절한 연결로 인하여 취약성을 나타내게 된다. 따라서 보안은 기술의 문제이기 보다 우선적으로 경영의 문제가 된다.

품질은 ISO8402에 정의되어 있듯이 고객의 요구를 충족시키는 제품의 특성이라는 측면에서 기본적으로 제품에 대한 품질로서 이해될 수 있다. 그러나 이와같은 제품 품질은 실제로 제품을 생산하는 프로세스에 크게 영향을 받으며, 프로세스를 잘 경영하는 것은 제품 품질을 확보하는데 필수적이다. 또한 프로세스를 지속적으로 개선할 경우 이 프로세스에 따라 생산되는 제품의 품질이 더욱 향상될 수 있다는 측면에서 프로세스 품질은 중요시되고 있다. ISO9000 serics는 이와같은 개념하에서 모든 산업에 적용가능한 프로세스를 식별하고 표준화한 것이다. ISO9001은 프로세스에 대한 품질경영을 위하여 품질시스템을 구축할 것을 요구하면서, 품질시스템에 대한 요구사항을 <표 1>과 같이 규정하고 있다[7].

<표 1>은 일반적인 품질시스템에 대한 요구사항이며 소프트웨어에 대하여는 ISO9000-3이라는 특별한 해석이 제공되고 있다[8] ISO9000-3 해석은 소프트웨어 생명주기를 개발프로세스에서 중요한 특성으로 인식하고, 모든 품질시스템 요소를 품질시스템 체계, 생명주기 활동, 지원활동으로 구분하여 설명하고 있다. ISO9000-3은 보안 체계를 구성하는 기초로 활용될 수 있다. 이러한 점에서 비교해 볼때 ISO9000-3에서 규정한 품질시스템 요소와 보안 체계에서 요구될 수 있는 요소들을 같이 비교하여 생각해 볼 수 있으며, <표 2>는 이러한 비교를 제시하고 있다.

체계 골격에서 보안 측면에서 필요한 활동들은 경영자가 체계를 수립하고 주기적 감사를 통하여 체계를 유지하는 점에 초점이 맞춰져 있다. 경영자는 우선 보안방침을 수립하여 조직 전체 차원에서 보안에 대한 방향과 의지를 표명하고, 이러

<표 1> 품질시스템 요구사항

항 목	설 명
4. 품질시스템 요구사항	
4.1 경영자의 책임	- 품질방침 - 조직 - 경영자에 의한 재검토
4.2 품질시스템	- 문서화된 품질시스템 확립, 유지
4.3 계약내용의 재검토	- 계약내용 확인, 활동절차 확립
4.4 설계관리	- 일반 - 설계 및 개발의 계획 - 설계에의 입력 - 설계로부터의 출력 - 설계 검증 - 설계변경
4.5 문서관리	- 문서의 승인 및 발행 - 문서의 변경.개정
4.6 구매	- 일반 - 외주업체의 평가 - 구매 데이터 - 구매품의 검증
4.7 구매자 공급품	- 납입제품에 편입되는 구매자 공급품의 검증, 보관, 유지 절차 확립
4.8 제품의 식별 및 추적성	- 제품 식별 및 추적성 확립을 위한 절차
4.9 공정관리	- 일반 - 특수 공정
4.10 검사 및 시험	- 구입 검사 및 시험 - 공정내의 검사 및 시험 - 최종 검사 및 시험 - 검사 및 시험의 기록
4.11 검사, 측정 및 시험의 장치	- 규정된 요구사항에의 적합 판단
4.12 검사 및 시험의 상태	- 제품의 검사 및 시험 상태 식별
4.13 부적합품의 관리	- 부적합품의 식별, 문서화, 평가 - 부적합품의 재심 및 조치
4.14 시정조치	- 부적합품의 원인 조사 및 시정조치
4.15 취급, 보관, 포장 및 인도	- 절차 확립, 문서화 유지 - 손상 방지 취급 방법 설정 - 손상 방지하는 보관 방법 설정 - 포장, 보존처리 및 표시방법 관리 - 인도 전까지 품질보호 대책 강구
4.16 품질 기록	- 품질기록 식별, 수집, 보관, 유지 절차
4.17 내부 품질감사	- 품질시스템의 유효성 판단을 위해 내부 품질감사 운용
4.18 교육.훈련	- 교육.훈련 절차 확립 - 업무 종사자 자격 인정
4.19 서비스	- 서비스 절차 확립
4.20 통계적 수법	- 공정능력 및 제품특성의 합격여부 검증을 위해 통계적 수법 사용

<표 2> ISO9000-3 해석에 의한 품질시스템 요소와 보안체계 요소의 비교

	ISO9000-3 해석에 의한 품질시스템 요소	보안 체계 요소
체계 골격	- 경영자 책임 - 품질 시스템 - 내부 품질시스템 감사 - 시정조치	- 보안방침, 보안조직, 보안관리 프로세스 - 보안표준, 지침, 절차서 - 보안 감사 및 시정조치
생명주기활동	- 계약 검토 - 구매자 요구사항 규격 - 개발계획 - 품질계획 - 설계와 구현 - 시험과 검증 - 검수 - 유지보수	- 보안 요구사항 관리 - 보안 계획 - 보안 설계와 구현 - 보안 시험과 검증 - 보안 사고관리 및 비상계획 - 주기적 보안 위험 평가
지원활동	- 구성관리 - 문서통제 - 품질기록 - 측정 - 규칙, 관행 및 실무 - 도구와 기법 - 구매 - 포함된 소프트웨어 제품 - 훈련	- 보안대책 구성관리 - 보안문서 통합 관리 - 보안 기록 - 보안 위험 측정 - 보안 규칙, 실무 - 보안 도구와 기법 - 보안제품 구매 - 포함된 보안 소프트웨어 제품 - 보안 교육/훈련, 인식제고

한 방침에 근거하여 보안 표준, 지침, 절차서를 수립하게 된다. 이러한 보안 표준, 지침, 절차서는 생명주기활동이나 지원활동에서 식별된 프로세스별로 작성되며, 이러한 문서들은 실제 활동을 수행할때 근거되는 문서이며 또한 보안 감사시 기준으로도 활용되게 된다. 감사에서 지적된 사항들은 해결을 위하여 지속적으로 관리되어야 하며, 장기간 해결되지 못하는 문제는 상위 관리자에게 보고되어 해결방안이 모색되어야 한다.

생명주기활동은 주로 시스템 개발과 운영과 관련된 사항으로 생명주기에 따라 필요한 프로세스들이 식별되어 있다. 보안 요구사항은 시스템 기능 요구사항과 독립적으로 관리될 필요가 있으면, 통합적으로 분석되어 적절성이 판단되어야 한다. 이를 기초로 보안계획이 수립되고 계획에 따른 감독이 수행되어야 한다. 보안 요구사항은 설계되어 구현되고, 요구사항을 만족하는지 여부를 시험과 검증을 통하여 증명되는 것이 필요하다. 운영시에는 보안 사고관리 및 비상시 업무 수행을 가능하게 하고 정상상태로 복구하기 위한 비상계획의 수립이 필요하다 또한 주기적 보안 위험을 평가하고 적절한 보안성을 유지하기 위한 노력도 필요하다. 이러한 생명주기활동은 보안의 목적을 달성하기 위한 핵심 프로세스이며 이를 지원하는 지원활동도 필요하다.

지원활동에는 ISO900-3에서 제시되는 모든 프로세스가 적용가능하다. 다만 보안 측면에서의 독립적이고도 통합적인 노력이 필요하다. 보안은 시스템 측면에서 볼때 시스템의 구성요소에 산재해 있고(예를 들면 데이타베이스 보안, 응용 보안,

운영체계 보안, 통신 보안 등), 또한 시스템에 내재되는 보안대책들은 관리적 절차들과 밀접한 관계가 있다. 즉 패스워드 시스템의 경우 사용자의 식별과 인증 서비스를 위하여 흔히 사용되나, 이러한 시스템이 패스워드 관리의 부적절로 무력화되는 경우가 흔히 있으며, 이러한 위험을 방지하기 위해선 패스워드 관리 절차의 수립과 준수가 필요하게 된다. 따라서 지원활동은 생명주기활동과 밀접한 관련을 가져야 하며, 이를 수행하기 위한 독립적이고도 통합적인 노력이 필요하다.

4. 보안관리 능력 향상을 위한 단계별 접근방법

보안관리 능력 향상을 위해서는 <표 2>에서 제시된 보안관리 프로세스를 적용하는 것이 필요하나 조직의 환경에 따라서는 단계적으로 향상하는 것이 바람직 할 수 있다 단계별 향상을 위해서는 우선 제시된 프로세스를 조직 환경에 맞게 조정하고 우선순위를 정하여 단계별로 향상할 수 있는 적용계획을 수립하는 것이 필요하다. 최근 국제적으로 정보기술 보안관리를 위하여 표준을 수립하고 이러한 표준에 대한 준수여부를 평가하여 인증하여 주는 체계 수립에 대한 노력이 기울여지고 있다. 영국의 경우 이미 국가표준으로 BS7799(1995) 정보보안관리를 수립하고 이에 대한 인증을 DNVQA에서 TrustIT이라는 서비스로서 제공하고 있다[9]. 영국은 BS7799를 국제표준화단체인 ISO에 제출하여 국제 표준화 작업을 하고 있다. BS7799는 35개의 필요한 통제를 설정하고 이중 10개는 필수 통제로 제시하고 있다. DNVQA의 TrustIT 인증서비스는 이를 기초로 보안관리 능력의 성숙도 수준에 따라서 4가지 수준으로 구분하여 인증을 하고 있다. <표 3>은 TrusIT 인증서비스의 수준을 보여주고 있다. TrustIT 인증서비스는 우선적으로 주요통제를 중심으로 인증서비스가 구성되어 있으며 주요통제만 만족하더라도 Level 2에 까지 이를수 있는 것으로 정의되어 있다. BS7799의 주요통제는 ISO9000-3에 따른 보안체계요소와 비교해 볼때 매우 적은 부분만을 포함하고 있으며, 관리 프로세스 관점에서의 정의가 미흡한 것으로 보인다. <표 4>는 ISO9000-3에 따른 보안체계요소와 BS7799의 주요통제를 비교하고 있다.

<표 4>는 본 논문에서 제시하는 보안체계요소와 BS7799의 주요통제를 비교적 관련성이 높은 항목끼리 연결하여 보여주고 있다. 체계 골격 측면에서는 보안방침의 수립이나 책임의 할당과 조직구조의 수립, 보안감사를 통한 보안방침의 준수여부 평가 등이 포함되어 비교적 일치되는 것으로 볼 수 있다. 그러나 생명주기활동과 지원활동에서는 상당히 특정 이슈만을 통제로 설정하여서 관리프로세스 측면이 강조되지 못하고 있는 것으로 보인다. 즉 조직의 주요기록을 보호하기 위한 것이나, 개인정보를 보호하기 위한 것은 보안요구사항의 일부이며, 소프트웨어나 하드웨어를 보호하는 것이 고려되지 못하고 있다 이는 보안 요구사항 관리라는 프로세스적 측면에서 접근하기 보다는 요구사항의 대상중 특정 이슈를 통제로 설정하므로서 발생되는 문제이다 본 논문은 특정 이슈보다는 관리프로세스가 중요함을 강조하고, 이슈들은 조직의 환경이나 방침에 따라 자주 변경될 수 있는 것으므로 실제 프로세스를 적용하면서 분석되어야 할 대상으로 보고있다. 따라서 BS7799는 현실적으로 당장 적용가능은 하나 장기적으로 보안체계를 수립하고 유지한다는 점에서는 미흡한 것으로 보이며, 본 논문에서 제시된 보안관리 프로세스 측면에서의 연구와 발전이 향후 이루어 지길 기대한다.

5. 결 론

정보화시대에 보안은 가장 중요한 문제점으로

<표 3> DNVQA의 TrustIT 인증서비스 수준

수 준	설 명
Level 0 Not Performed	보안대책이 거의 없으며 관리의지도 없음
Level 1 Performed Informally	주요통제의 일부가 수행되고 있으나 엄격하지 못함
Level 2 Fundamental	주요통제가 전부 효과적으로 수행되고 있음
Level 3 Defined	주요 위험이 식별되고 적절한 통제에 대한 관리적 결정이 이루어짐

<표 4> ISO9000-3에 의한 보안체계요소와 BS7799의 주요통제 비교표

	보안 체계 요소	주 요 통 제
체계골격	- 보안방침, 보안조직, 보안관리 프로세스 - 보안표준, 지침, 절차서 - 보안 감사 및 시정조치	- 정보보안방침 - 정보보안 책임의 할당 - 방침에의 준수
생명주기활동	- 보안 요구사항 관리 - 보안 계획 - 보안 설계와 구현 - 보안 시험과 검증 - 보안 사고관리 및 비상계획 - 주기적 보안 위험 평가	- 조직기록의 보호 - 개인정보보호 - 보안사고보고 - 사업연속기획
지원활동	- 보안대책 구성관리 - 보안문서 통합 관리 - 보안 기록 - 보안 위험 측정 - 보안 규칙, 실무 - 보안 도구와 기법 - 보안제품 구매 - 포함된 보안 소프트웨어 제품 - 보안 교육/훈련, 인식제고	- 소프트웨어 불법복제 - 바이러스 통제 - 정보보안 교육/훈련

대두되고 있다. 특히 최근 우리나라에서는 산업정보화를 위하여 CALS를 도입하여 구축하는 노력이 많이 기울여지고 있다. 이러한 시기에 개발초기부터 보안을 고려하여 시스템을 구축하는 노력이 필요하며, 이는 단순히 기술적 노력뿐만 아니라 관리적 노력이 우선적으로 필요하다. 본 논문은 보안의 문제가 기술적 문제이기 전에 관리적 문제임을 강조하고, 보안관리를 프로세스 측면에서 분석하여 보안관리체계를 수립하고자 하였다. 특히 ISO9000에서 제시되는 품질시스템에 기초하여 보안관리 프로세스를 식별하였고, 이를 현재 표준으로 수립되어 있는 BS7799와 비교분석하여 프로세스적 접근방법이 장기적으로는 필요할 것임을 설명하였다. 향후 보안관리 프로세스에 관한 연구와 토론이 활발히 일어나기를 바라며, CALS와 같은 주요한 시스템 구축노력에서도 본 논문에서 제시된 개념들이 발전되어 적용되기를 기대해본다.

참고문헌

[1] 신장균, 나민영, 이승희, CALS 구현을 위한 정보기술, 정보과학회지, 제13권 제11호, pp. 5-16, 1995.

[2] Charles C. Wood, Effective Information Security Management, Elsevier Advanced Technology, 1992.

[3] ISO/IEC DTR 13335-1, Guidelines for Management of IT Security - Part 1 : Concepts and Models for IT Security, 1995.

[4] CCTA, Guidelines for Directing Information Technology Security, HMSO, 1991.

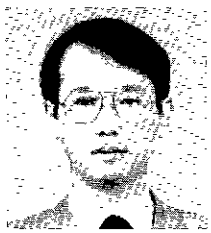
[5] ISO9000/KSA9000, Quality Management and Quality Assurance Standards - Guidelines for Selection and Use, 1992.

[6] ISO8402, Quality Management and Qualtiy Assurance-Vocabulary, 1994

[7] ISO9001/KSA9001, Quality System-Model for Quality Assurance in Design/Development, Production, Installation and Servicing, 1992.

[8] ISO9000-3, Guideliens for the Application of ISO9001 to the Development, Supply and Manintenance of Software, 1992.

[9] BS7799, Code of Practice for Information Security Management, 1995.



신 동 익

1978년 고려대학교 식품공학과 졸업 (학사)
1984년 오하이오대학교 경영학과 회계학 전공 졸업(석사)
1991년 네브라스카대학교 경영정보학 졸업(박사)

1997년 현재 한국전산원 감리본부 책임연구원
관심분야 : 정보기술 감사 및 평가, 소프트웨어 공학, 정보보호