情報保護學會論文誌
第18卷 第5號, 2008. 10

기업의 정보보호수준 측정모델 개발에 관한 연구

이 희 명†, 임 종 인‡
고려대학교 정보경영공학전문대학원

A Study on the Development of Corporate Information Security Level Assessment Models

Hee-Myung Lee†, Jong-In Lim‡
Graduate School of Information Management and Security, Korea University

요 약

최근 첨단기술과 핵심정보의 불법적인 유출 및 해킹과 바이러스 등으로 인한 피해사례가 계속 증가하고 있으나, 기업에서의 보안사고 방지와 예방체제는 아직도 미흡한 편이다. 대기업을 중심으로 회사의 중요한 정보를 보존하기 위한 장치로써 정보보호관리체계(ISMS)를 도입하여 운영하고 있으나, 기존의 정보보호수준 진단 및 측정 모델은 주로 ISO 27001에 기반을 둔 정보보호정책과 제도의 수립여부, 또는 IT 분야에 초점을 둔 지표 중심으로 평가를 함으로써 기업의 전반적인 보안수준 평가와 보안사고 예방체제 강화에는 부족한 점이 많았다. 본 논문에 소개 된 정보보호수준 측정모델은 기존의 정보보호관리체계는 물론, 정보보호활동의 성과를 정량적으로 평가하여 각종 보안사고의 예방 및 대응방안 수립에 활용 가능하도록 국내외 사례연구와 함께 경영관리기법으로 많이 사용되고 있는 BSC(Balanced Scorecard)를 적용한 실용성에 초점을 맞추어 개발하였다.

ABSTRACT

Despite the recent growth in size and frequency of damages caused by illegal information breaches, current business counter-measures and precautionary systems are greatly limited. Some major companies have developed Information Security Management Systems (ISMS) to safeguard their vital information; however, such measures are largely based on the ISO27001 and lacks in many aspects to grasp the holistic corporate security level and reinforce precautionary measures. The information protection level evaluation model introduced in this paper is a pragmatic evaluative tool that can be utilized to devise effective corporate information security precautionary measures and countermeasures, based on the BSC (Balanced ScoreCard) method for an actual and realistic corporate information security level evaluation possible.

Keywords : ISO 27001/27002/27004, BSC(Balanced Scorecard), ISMS

접수일 : 2008년 4월 21일; 수정일 : 2008년 6월 16일;
채택일 : 2008년 7월 31일
† 주저자, hmlee@posco.com
‡ 교신저자, jilim@korea.ac.kr

Ⅰ. 서 론

1.1 연구배경 및 목적

각 기업들은 급속한 IT 기술의 발달과 함께 해킹이나 바이러스, 이동식 저장기기(USB나 카메라 폰 등)의 확대로 기술보안의 취약점이 지속적으로 증대되고 있는 반면, 효율적인 정보보호 시스템의 구축과 운영에 상당한 어려움을 겪고 있다. 또한, 물질만능주의 및 개인주의가 인사 불만과 직장의 안전성 결여 등과 맞물려 회사에 대한 애착심이 약화되면서, 내부직원들이 사소한 유혹에도 회사의 기밀정보나 기술을 유출하는 범죄행위가 나타나고 있다.

일부 선진 기업에서는 정보보호관리체계(ISMS)를 도입하여 운영하고 있으나, 대부분이 문서화에 치우쳐 있고, 관리지표에 대한 정확한 인식의 부족 등으로 그 실효성에 의구심이 제기되고 있으며, 정보보호 활동의 정량적인 측정도 어려운 형편이다. 현재 ISO 27001 (ISMS Requirements,'05.8) 방법론에 의한 정보보호 수준 진단과 국제인증제도가 시행되고 있지만, 주로 관련규정의 문서화 및 일부 보안 주관부서 인력 위주의 심사를 통한 자격취득과 인증서 발급 등으로 일정기간의 시간이 지난 후에는 기업의 보안 수준이 다시 원점으로 회귀하는 현상마저 벌어지고 있다.

따라서 본 논문에서는 다양한 형태의 보안 취약점 발굴과 사전 예방체제의 확립을 위한 도구로써 객관적, 정량적인 방법으로 보안관리지표를 측정하고, 기업의 정보보호 수준을 종합적으로 평가할 수 있는 정보보호수준 측정모델과 기준을 제시하고자 한다.

1.2 연구범위 및 방법

정보보호의 관리대상과 범위는 단순한 출입관리나 시설보안점검, 또는 해킹이나 바이러스로부터 시스템의 안정적인 운영환경을 조성하는 수준에서 벗어나 내/외부인을 포함한 사람 중심의 인적보안은 물론, 심지어 테러나 천재지변에 의한 총체적인 위험관리에 이르기까지 다양한 정보자산의 취약성 분석을 통한 구체적인 위험대응방안을 수립하여 종합적이고 체계적인 정보보호 활동의 수준까지 지속적으로 확대해 나가야만 한다.

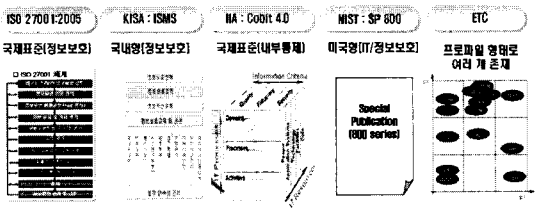
이러한 점을 고려하여 본 논문은 기존 정보보호 관리체계의 적용사례를 통해 문제점과 개선방안을 살펴보고, 기업의 정보보호수준을 정량화하여 지속적인 정보보호 관리체계가 정착화 되도록 각 보안영역별로 관리지표를 선정한 후 정량적 측정 모델을 기반으로 정보보호수준을 실제로 측정해 본 결과까지를 포함한다. 이를 위해 정보보호 수준측정에 관한 국내외 사례를 분석하였으며 현대 경영관리기법으로 널리 사용중인 균형성과지표(BSC, Balanced Scorecard)를 활용하여 정보보호 성과지표를 도출하고 측정하는 과정을 포함하고 있다.

Ⅱ. 기존 측정모델의 운영사례 분석

2.1 국내외 기업의 운영사례

오늘날 기업에서는 중요한 정보자산을 보호하기 위하여 정보보호관리체계방법론(정보보호 정책 및 제도, 정보자산 분류 및 위험평가, 보안조직 및 변화관리교육, 보안통제 및 개선 활동 등)을 도입할 필요성을 느끼게 되었으며, 현재 ISO 27001이(ISMS Requirements, '05.8) 국제표준으로 제정되어 가장 널리 사용 되고 있다.

이와 유사한 개념으로는 SP800-53 (NIST,'06.12), COBIT4. x (ISACA,'07.5) 등 국가와 조직별로 다양한 모델이 응용되어 사용되고 있으며, 일본, 영국 등 해외 다수의 국가에서 ISO 27001를 국가표준으로 채택하여 정보보호인증(Certification) 제도와 컨설팅(consulting) 서비스 형태로 정보보호관리시스템을 도입하여 운영하고 있다. 아래 그림은 현재 대표적으로 활용되고 있는 다양한 정보보호관리체계 및 운영사례를 보여 주고 있다.



〔그림 1〕 정보보호관리체계방법론 국내외 운영사례

2.1.1. ISO27001 국제인증사례

우선 정보보호수준의 측정기준으로 가장 널리 사용되고 있는 ISO27001의 사례를 살펴보면, 각 보안영역별로 관리수준을 진단하여 일정수준 도달시 인증서를 발급(전체 100% 기준 대비 85% 이상, 중대한 결함이

없는 경우) 해 주는 제도로써, 총 11개 도메인과 133개 통제항목으로 구성되어 있다. 그러나, 이 제도는 각 통제항목별로 명확한 평가기준이 정의되어 있지 않기 때문에, 평가자와 피평가자의 주관적 판단에 따라 평가결과가 다를 수 있기 때문에 각 기업에서 적합한 세부평가 기준(부서, 평가 유효범위, 증빙형태)을 별도로 마련해야 한다.

또한 통제항목의 세부평가 기준은 Planning(기획, 계획)과 Execution(실행, 결과)으로 분류되어야 함에도 불구하고 하나의 통제항목에서도 평가 및 적용 대상부서(개별부서, 전사 적용여부)에 따라 관리기준이 다양화 될 수 있기 때문에 평가결과가 상이하게 나타날 수 있다. 아직까지는 보안정책과 제도의 수립여부 진단 등 문서를 통한 관리 및 계획 측면이 강한 반면, 보안실천수준의 진단기능이 약하기 때문에 실질적인 기업의 보안수준을 측정하기에는 한계점을 지니고 있다.

아래의 표는 ISO27001의 통제항목으로 현황진단을 수행하는 예시를 보여주고 있다.

〔표 1〕 ISO27001 통제항목의 예시

도메인	통제항목	평가	상세내용	증빙자료
보안정책 (A.5)				
정보보안정책 (A.5.1)	정보보호 정책문서	Y	사규등록	정보보호팀
	정보보호 정책의 검토	Y	상동	A부서 B부서
중간생략				
인적자원보안(A.8)				
고용전(A.8.1)	역할 및 책임	N		
	심사	N		
11 도메인	133개			

2.1.2 국내기업의 운영사례

정보보호수준 측정에서의 모호한 문제점을 개선하기 위하여 다양한 연구가 진행되고 있다. 현재 ISO 27004는 Draft 단계에서 발전하고 있으며 SP 800-55에서는 도메인별 평가기준을 적용하여 수준을 측정하고 하고 있으나, 아직은 다양한 고려요소를 지닌 기업에 직접적으로 적용하기에는 곤란한 형편이다. 또한, 이를 보완하기 위한 방법으로 몇 몇 국내기업에서는 각 각의 보안영역별로 정보보호 관리지표를 개발하여 활용하고 있다.

〔표 2〕 국내기업(B사) 측정지표 운영사례

구분	통제항목	측정지표
보안 정책	보안정책이해도	개정 보안정책에 대한 이해도
자산 분류 및 통제	자산목록 점검율	자산목록 점검횟수(연2회)
인적 보안	보안교육 실행율	연간계획 대비 실적
통신 및 운영 관리	시스템 변경점검 실행율	변경이력 점검횟수(연1회)
접근 통제	보안정책변경서 반영율	정책변경요청서와 시스템과의 일치성 점검횟수
	계정검토 실시율	주기적인 계정검토 횟수(연2회)
	원격접근 부정 사용율	지정관리자에 의한 사용내역 감사지적 건수
시스템 도입,개발 및 유지보수	보안성 검토 처리시간	보안성 검토 접수시점부터 통보시점까지 걸리는 시간
	취약점 수정 이행율	조치계획대비 이행율
보안사고 관리	동종사고 발생율	과거 발생한 동일사고 발생율
사업 연속성 계획	비상복구시간 달성율	비상복구목표시간대비 실제복구시간

B사의 경우, 위 표의 예시처럼 ISO27001에 기반을 두고 금융회사의 특성을 고려하여 특히, 시스템의 접근통제와 보안사고 관리 및 사업의 연속성 강화에 초점을 맞춘 통제항목(11개)과 측정지표(11개)를 중심으로 정보보호지표 관리체제를 운영하고 있다.

〔표 3〕 국내기업(D사) 측정지표 운영사례(일부)

구분	통제항목	측정지표
위험 관리	보안위협/취약성 정보 확보	위협/취약성 DB 업데이트(월간)
	보안위험평가 및 위험관리체계유지	위험관리시스템의 DB 업데이트(월간)
물리 보안	보안구역 운영관리	출입대장 관리내역 점검(주간) 반입PC점검대장 관리내역 점검(주간)
	시설 및 설비보호 활동	
	반출입통제 증적 이행	
사고 관리	침해사고 대응의 적절성	침해사고처리보고 증적 업데이트 ESM 관리보고 증적 업데이트

구분	통제항목	측정지표
On -line	보안사고 예방율	ESM 관리증적 vs 월간보안관리 보고증적비교(월간)
	보안사고 탐지율	
	보안사고 대응율	
보안 통제	인증/인가 업무수행여부	보안서버 증적관리 업데이트(월간) 취약성점검/대책적용 보고 업데이트(월간)
	접근통제 증적 이행여부	
	암호화 증적 이행여부	
	가용성 확보 증적관리	
	보안설정 변경 증적관리	
보안 운영	계정관리 취약성 조치여부	취약성점검/대책적용 보고 업데이트(월간) 백업관리 증적 업데이트(주간)
	보안성 검토내역 관리	
	취약성 점검 결과 이행	
	패치관리 결과 이행	
	모니터링/로그분석	
	백업/복구 이행결과	

D사의 경우, 위 표의 예시처럼 통신업체의 특성에 맞게 네트워크 부문의 이행도 측정에 중심을 두고 30개의 통제항목과 49개의 측정지표를 선정하여 운영하고 있다. 즉, 통신 서비스의 효율성을 제고하기 위한 보안영역별 통제항목을 선정한 후, 각 각의 통제항목별로 측정지표를 개발하여 타사 대비 체계적이고, 정량적인 정보보호 지표 관리체제를 운영하고 있으나, 세부 측정항목은 주로 IT 중심의 보안관리수준에 머무르고 있는 형편이다.

다음은 국내기업들의 정보보호 관리지표 운영사례를 종합적으로 요약한 내용이다.

〔표 4〕 국내기업(A, B, C, D사) 관리지표 운영사례
(범례 : ○ 수작업 ◐ 일부 자동화 ● 자동화 × 지표없음)

구분	통제 구분	지표수	IT 부서	일반 사용자	기술 연구소	해외 사업장
A사 (IT 업체)	관리	100 여개	●	●	●	●
	물리		×	×	×	×
	기술		●	●	●	●
B사 (금융 회사)	관리	3	○	×	×	×
	물리	0	○	×	×	×
	기술	8	○	×	×	×
C사 (제조 업체)	관리	30(5)	◐	◐	◐	◐
	물리	20	◐	◐	◐	◐
	기술	130	◐	◐	◐	◐
D사 (통신 업체)	관리	21	◐	×	×	×
	물리	3	◐	×	×	×
	기술	25	◐	×	×	×

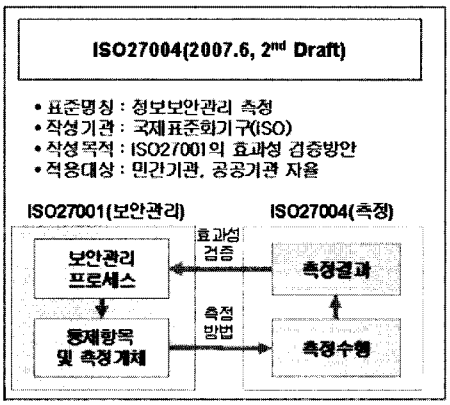
상기의 예처럼 몇 몇 기업에서 정보보호관리지표를 사용하여 정보보호수준을 측정하고 있으나, 측정항목의 대상과 범위 및 항목수가 많은 차이를 보이고 있다. 또한 측정방법도 아직은 자동화단계에 이르지 못하고 있으며, 측정되는 지표항목도 주로 IT 기술 중심의 일부 영역에 국한되어 있기 때문에, 종합적인 정보보호수준 측정에는 한계성을 지니고 있는 형편이다.

상기에서 살펴본 4개사(A, B, C, D사)의 사례를 종합해 보면, 특정 보안영역과 통제항목에 대해서는 관리지표를 선정하여 운영하고 있으나, 보안영역 전체를 포괄한 종합지표 형태의 정보보호수준 측정에는 아직 도달하지 못하고 있다.

또한 대부분 보안영역별(관리,기술, 물리보안)로 결과중심의 지표선정과 관리형태로 가장 기초적인 정보보호 관리체계(보안 규정 및 프로세스의 명확화, 보안시스템의 기본적인 아키텍처 구성 등)의 구축 및 운영실태가 상당히 취약한 편이다.

2.1.3 해외기업의 운영사례

다음은 해외사례를 살펴보고자 한다.

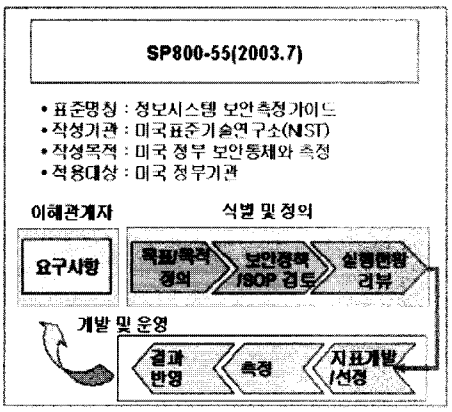


〔그림 2〕 ISO27004 운영사례

위 그림의 사례는 최근 해외의 민간 및 공공기관에서 기존의 ISO27001의 취약점인 보안수준 진단 및 평가부문을 개선하기 위하여, 보안관리 프로세스와 통제항목에 대한 측정을 통하여 실질적인 보안활동의 개선효과를 평가하는 예시를 보여주고 있다.

또한 아래 사례는 미국의 정부기관에서 사용하고 있는 NIST(미국표준기술연구소)에서 제정한 보안진단 툴

로써, 각 이해관계자의 요구 사항을 분석하여 보안정책과 프로세스 및 측정지표를 개발한 후 주기적인 측정 및 평가를 통한 지속적인 개선활동 등 일련의 보안활동 사이클을 보여주고 있다. 그러나, 전반적인 관리지표의 선정과 측정기준의 구체성은 아직도 미흡한 편이다.



〔그림 3〕 SP800-55 운영사례

2.2 기존모델의 한계점

기존의 표준 및 모델들은 정보보호관리시스템의 필요사항(Requirements)을 잘 정의하고 있으며 어느 조직에서도 적용 가능한 일반적이며 범용적인 특성을 가지고 있다. 그러나, 표준을 적용하기 위한 방법론 부족으로 흔히 정보보호관리시스템 도입이 정책 및 문서(Policy and Document)가 작성되는 수준으로 한정된다. 또한, 어렵게 도입된 정보보호관리시스템을 지속적으로 운영하기 위해 필요한 비용(인력, 시간, 예산) 및 정량적인 운영결과에 대한 효과적인 분석방법 역시 부족한 형편이다.

정보보호관리시스템(ISO27001) 인증제도에서는 정보보호 현황진단 및 일반적인 감사기법을 활용하여 적용성 보고서(SOA ; Statement of Application)를 작성한다. 그러나, 감사행위의 보증수준(Assurance level)은 기대치와 상이할 수 있으며 심사원 및 심사환경에 따라 결과가 다를 수 있다. 또한, 인증제도에서는 경영진 인터뷰를 통해 효과적인 커뮤니케이션을 시도하고 있지만 심사결과(SOA)가 서술식이고 정량적인 표현이 곤란하여 정보보호 전문지식을 보유하지 않은 경영진에게는 효과적이지 않다.

또 다른 진단방법인 정보보호관리시스템(ISO27001) 컨설팅 서비스에서는 통제항목(ISO 27001 Controls)을 중심으로 정보보호 현황진단을 실시하고 취약성 분석을 통해 계량화 된 보고서가 작성된다. 하지만, 세부적인 정보보호 현황진단을 위한 정보보호 통제항목(ISO 27001 Controls)의 구체화는 비용과 pay-off를 발생시키며 통제항목별 평가결과(Yes, No, Partial, N/A)는 구체적인 기준과 방법이 부족하여 컨설턴트 및 주변환경에 따라 결과가 만족스럽지 못 할 수 있다.

현재 이러한 요구사항을 기초로 하여 실질적인 보안수준의 개선 및 측정을 위한 ISO 27004(ISM Measurements)가 작성중이나, 아직은 Draft 단계에 있다. 또한 SI 분야에서는 정보보호 위험관리시스템이 개발되고 있으나 대상분야가 IT분야(기술적 보안) 및 위험(Risk)기반으로 제한되어 포괄적(관리, 물리, 기술) 이고 적극적(Proactive) 차원의 정보보호 활동 및 정보보호 수준관리의 개념과는 차이가 있다.

Ⅲ. 신규모델의 설계방법론 및 종합구성도

3.1 프로세스 관점의 설계

본 연구에서는 앞서 기존 모델에서 기술된 문제점들에 착안하여, 정보보호관리체계의 개선방안을 수립하는 동시에 정보보호수준 측정모델을 설계해 나가고자 한다.

정보보호수준 측정모델의 설계에 앞서 우선 2가지 개념을 명확히 하고자 한다. 첫째, ISO27001(ISMS Requirements)에서는 정보보호 관리체계를 도입하여 운영할 때, PDCA(Plan- Do-Check-Act)의 과정을 통한 지속적인 개선을 요구하고 있다.

둘째, 각 기업은 ISO27002에서 제시하는 정보보호 요건을 무조건적으로 도입하기보다는, 기업의 특성과 조직내부에 적합하도록 실행과 측정이 가능한 형태로 변환하여 적용하여야 한다.

이러한 2 가지 개념을 전제로, 각 기업에 적합한 프로세스를 최적화해야 한다는 핵심결론을 도출하였으며, 프로세스 기반의 측정모델을 설계하였다.

첫째, 기존의 정보보호 수준측정에서 통제항목 적용시, 평가자(컨설턴트 등)간의 측정기준 차이를 프로세스 접근방식을 사용함으로써 해결하였다. 정확하고 객관적인 수준측정을 위해 평가자는 평가대상을 정확히 이해한 후, 실제로 기업에 어떻게 보안통제가 적용되고 있는지 측정을 해야 한다. 기업에 따라서는 통제항목 A가 여러가지 형태로 적용될 수 있기 때문에 평가대상에 대한 정확한 이해와 함께 동일한 평가기준이 수립되어

야 한다. 따라서 특정 프로세스와 관리지표를 측정할 경우, 평가자 모두가 평가기준과 평가과정상 프로세스 절차를 정확히 이해할 수 있도록 통제항목, 관리지표, 프로세스간 상호 연계성을 갖도록 측정에 앞서 개념정의를 명확하게 해 두어야 한다.

둘째, 보안지표가 일부 영역에 국한되어 적용되는 문제점을 해결하기 위하여 지표 Pool을 구성하고 측정된 값이 대표성을 지닐 수 있도록 프로세스와의 연계성을 강화하였다.

보안지표는 현재의 보안수준을 Sampling하는 개념이기 때문에 많을수록 좋은 것이 사실이다. 그러나, 현실적으로 많은 지표를 운영하기 위해 수반되는 인력이나 비용의 부담 때문에 적당한 수준에서 관리지표를 선정하여 운영해야만 한다. 이러한 문제점을 해결하기 위하여 지표 Pool을 통해 한계수치를 모니터링 하거나 핵심지표를 선정하는 방법을 병행함으로써 특정 영역에 집중되는 관리지표의 쏠림 현상을 방지하고 대표성을 유지할 수 있게 설계하였다.

셋째, 정보보호수준 측정모델의 객관성을 확보하기 위한 정량화는 기업의 정보보호관리체계를 직접 운영하는 주관부서인 보안관리자 파트와, 실제 정보보호기준을 실천하고 준수하는 임직원 파트를 구분하여 각 대상별로 운영 모델을 제시하였다.

3.2 BSC 관점의 균형관리

또한 현재 최신 경영관리기법으로 널리 사용되고 있는 균형성과지표(BSC, Balanced Scorecard) 방법론을 정보보호 관리지표 설계와 기준 정립에 활용하였다.

BSC는 경영성과를 높이기 위한 구체적인 전략을 수립하고 각 전략별 핵심 성과지표를 선정하여 주기적으로 측정 및 관리함으로써 효과적으로 경영목표를 달성해 나갈 수 있는 경영관리 툴의 일종이다. 즉, 기존의 전통적인 재무적 관점 중심의 경영관리에서 벗어나, 최종적인 경영의 목표를 달성해 나가는 각 과정을 4단계로 구분하여(학습 및 성장 관점 → 내부 프로세스 관점 → 고객 관점 → 재무 관점), 전략과의 일치성에 초점을 두고 지표간의 연계성을 유지하는 동시에 장단기적인 균형성을 고려한 종합적인 경영관리기법이다.

이러한 BSC 이론을 응용하여 본 정보보호 측정모델을 설계하면서, 3가지의 구성요소로 종합지표를 구성하였다. 먼저, 가장 기본이 되는 기반지표는 기업의 정보보호체계를 각 영역별로 측정하기 위한 원칙과 기준을 중심으로 지표를 선정하였으며, 이행지표는 실제 업무 수행과정에서 정보보호 규정이나 프로세스를 실천하는 정도를 측정할 수 있는 지표를 선정하였고, 마지막으로 결과지표는 기반지표와 이행지표의 최종결과로써 나타나는 보안수준의 결과치를 보여줄 수 있는 지표를 선정하였다.

3.3 신규모델의 설계방법론

신규모델에서는 먼저 측정대상 지표 POOL을 설계한 후, 개별 지표단위로 정의서를 작성하고, 각 보안영역별로 측정 및 평가를 실시하는 단계별 절차를 따르고 있다.

3.3.1 지표 POOL 설계

아래의 표는 3가지 지표영역별(기반지표, 이행지표, 결과지표)로 경영전략과 연계하여 선정된 지표 POOL 사례를 예시로 보여주고 있다.

〔표 5〕 영역별 지표 POOL 사례(일부)

기반지표	이행지표	결과지표
- 보안조직구조 구성/절차 - 자산분류 절차 정의 - 보안교육 R&R - 정보백업 절차 정의 - 보안모니터링 성숙도 - 서버접근통제 성숙도 - 기술취약점관리 절차 - 보안사고관리 절차 - 시스템감사 절차 정의	- 보안정책 검토율 - 보안위원회 개최율 - 제3자계약 보안성 검토율 - 외주파트너 PC 지급율 - 정보자산 갱신율 - 방화벽 로그 분석 실행율 - 시스템 위험 평가 실시율 - 로깅 설정 서버 비율 - 외부방문자 사무실출입율	- 악성코드 발생율 - 침해사고 발생 빈도 - 침해사고 조치 완료시간 - 모의해킹 취약점 발견율 - 출입증 분실 부서비율 - 보안징계발생 부서비율 - 보안교육 성취도 - 변경작업후 사고발생율 - 장애발생주기 (MTBF)

3.3.2 지표정의서 작성

다음의 표는 상기의 3가지 영역별 지표에 대한 관리기준과 평가기준을 정의한 구체적인 지표정의서 사례를 보여주고 있다.

〔표 6〕 지표정의서 사례(DRM 클라이언트 PC 설치율)

지표개요	지표명	DRM 클라이언트의 PC 설치율	지표코드	PSI-0001
	지표관련부서	OO 그룹	지표측정부서 (담당자)	정보보호팀
	지표목적	DRM설치가 되지 않은 PC의 비율을 높여서, 사내 문서의 원천암호화 완전성을 확보		
	지표관점	이행도	적용단위	부서KPI
	지표영역	기술적 보안	관련 ISO통제항목	ISO 11.3, 11.9
	관련규정지침	보안규정 제 XX조		
	실행자	전체부서		
	본지표가 영향을 받는 지표	PC내 비 암호화 파일 비율	본지표가 영향을 주는 지표	부서보안교육실시율
지표해설	계산식	DRM이 설치되지 않은 PC대수 * 100 부서 전체 PC대수		
	측정주기	주간	단위	%
	지표방향	상향	지표범위	0~100
	데이터 소유자	IT 보안팀 ***		
	데이터 원천	1. PC보안시스템 (메뉴 : 인벤토리관리->부서별 PC현황) 2. DRM 관리시스템		
	데이터 수집방법	PC관리시스템에서 등록 된 부서 PC대수와 DRM관리시스템의 부서별 등록대수를 IT 보안팀에서 매주 화요일 전 부서별로 취합하여 목요일 까지 엑셀파일 형식으로 정보보호팀 *** 에게 전달 함		
측정결과	현재값	98	현재표지	Yellow
	목표값	99	위험값	90
	목표 및 성과평가	기술문서 등 많은 내부데이터들이 비정형적으로 PC에 저장되어 있는 상태에서 원천암호화는 매우 중요함. 현재 98%의 설치 비율은 더 높여야 될 필요성이 있음.		
	전략실행과제	1. DRM Agent 일괄 자동배포실행 방안 검토 2. 각 부서 자율보안교육 교재에 반영		

3.3.3 측정방법의 설계

본 연구에서는 3가지 지표를 기반으로 측정모델을 구성하였으며, 각 지표의 측정은 PDCA 진단방법론을 기초로 5단계 수준진단에 의해 종합적인 평가를 하도록 설계하였다.

우선, 3가지 지표를 구체적으로 정의해 보면,

첫째, 기반지표는 정보보호 기반체계와 보안통제의 구축 수준을 측정하는 지표로써, ISO 27002(best practice)에 정의된 프로세스 관점에서 정보보호 활동체계, 정보보호 문화정착 등의 근간이 잘 구성되어 있는지를 평가하는 것이다. 또한, 5단계 수준평가(임의수행, 계획, 이행, 평가, 개선)를 통하여 활동의 성과를 측정하므로, 하위단계를 충족시키지 못하면 상위단계로의 진입은 불가능하며 보다 엄격하고 객관적인 평가를 하게 된다.

둘째, 이행지표는 개별지표의 실천으로 보안활동의 이행 수준이 향상되는 것을 측정하는 지표로서 규정이나 지침, SOP 등으로 구성되어 있으며, 보안수준이 높을수록 점수가 높아지게 된다.

셋째, 결과지표는 보안활동의 이행에 따른 보안사고의 감소 수준을 나타내는 지표로서, 수준 미달시 패널티 항목으로 적용되기 때문에 보안수준이 향상 될수록 차감 점수가 작아지게 된다.

이를 종합해 보면,

$$G = B + P - R$$

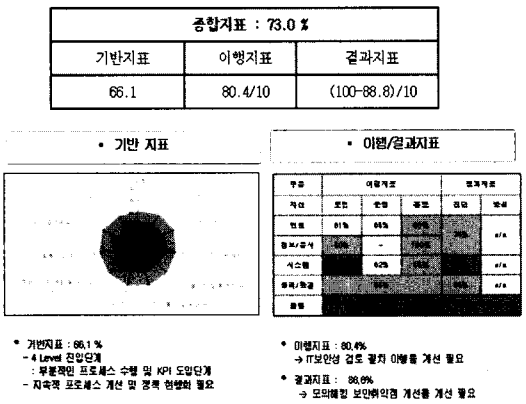
(각 기업의 정보보안 수준을 0~100의 값으로 평가하게 됨)

즉, 정보보안 종합지표(G)는 기반지표(B)+이행지표(P) - 결과지표(R)의 형태로 구성된다.

여기에서 결과지표의 값이 100%의 완벽한 수준에 도달하지 못할 경우, 보안사고 발생이나 위험성을 내포하기 때문에 감점요인으로 적용됨으로써, 기존 측정수단보다 엄격한 관리 형태로 운영되게 된다.

3.4 신규모델의 종합구성도 및 적용사례

아래 그림은 측정모델에 의한 진단과 평가를 실시한 결과를 보여 주고 있다. 우선 아래 그림은 종합지표로써, 기반지표, 이행지표, 결과지표의 평가점수를 합산한 결과치이다.



〔그림 4〕 측정모델 적용 사례

이러한 종합지표는 전사 보안주관부서에서 전사 차원의 보안수준 진단과 취약점 분석을 통한 개선활동에 활용하기 위하여 정량적 지표는 물론 일부 정성적 지표까지 포함하여 운영 및 관리를 하고, 일반 현업부서에서는 각 부서의 실질적인 보안수준을 정량적으로 측정한 이행지표와 결과지표를 중심으로 자체적인 관리와 개선활동을 해 나갈 수 있다. 특히, 기업에서 보안체계의 근본이라 할 수 있는 기반지표는 보안주관부서에서 가장 핵심지표로 관리하면서 지속적인 개선을 해 나가야 한다.

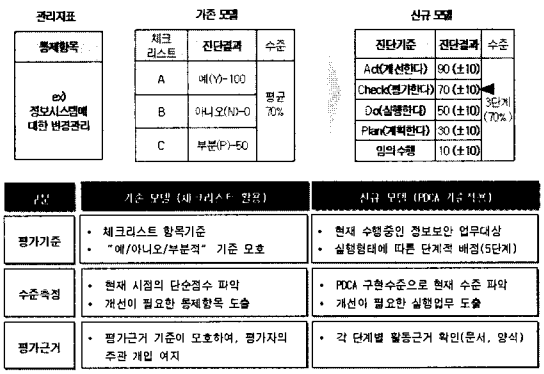
3.5 기존모델 대비 신규모델의 장단점

본 연구를 통해 소개된 정보보호수준 진단을 위한 신규 측정모델은 기존의 측정 및 평가모델과 대비하여 다음과 같은 차이점을 지니고 있다.

첫째, 기존 모델은 대부분 단순히 각 보안영역별(관리, 기술, 물리) 관리지표를 선정하고 운영함으로써 가장 기초적인 정보보호체계의 기반이 다소 미약하더라도 결과지표 중심의 평가를 통하여 일정수준 이상의 보안수준 평가점수를 획득할 수 있었다. 그러나 신규 모델에서는 보다 엄격한 3단계 모델 적용방법을 통하여 우선적으로 가장 기본적인 정보보호관리체계를 측정할 수 있는 기반지표를 선정하고 운영함으로써 보다 견실한 보안관리의 기반을 마련하고, 다음에 이행지표의 철저한 실행과 측정, 그리고 최종적인 결과로써의 보안사고 예방을 진단할 수 있는 결과지표를 종합한 평가제도를 통하여 명실상부한 정보보호수준을 명확히 알 수 있다.

또한, 각 지표영역별로 다양한 지표 POOL을 작성하여, 매년 주기적으로 새로운 경영여건의 변화에 따른 관리지표를 선정, 운영함으로써 보다 개관적이고 현실에 적합한 측정모델 형태를 갖출 수 있다.

아래의 그림은 기존 모델과 신규 모델의 정보보호수준 진단방법을 비교한 것이다.



〔그림 5〕 기존 모델 대비 신규 모델의 진단방법 비교

상기의 예처럼 기존 모델은 대부분 3단계 평가(관리항목별 적용, 미적용, 부분적용)방식으로 수준을 측정하여 빠르게 결과를 볼 수 있는 반면 정확한 진단이 어렵다. 또한 신규 모델에서는 보다 엄격한 5단계(관리항목별 임의수행, 계획, 실행, 평가, 개선) 방법으로 객관적인 수준 진단 및 평가가 가능하지만, 기존 모델 대비 기본 DATA의 수집 및 분석 등에 다소 시간이 소요되는 경향이 있다. 그러나, 이러한 문제점들은 선정지표의 관리기준을 명확히 정의한 후, 시스템과 연계된 데이터 수집과 이미 상용화 된 통계분석 툴 등을 이용한다면 쉽게 해결해 나갈 수 있다고 본다.

Ⅳ. 기대효과

본 연구에서 개발된 측정모델을 사용할 경우, 그 기대효과를 살펴보면,

첫째, 정보보호 수준진단을 통해 정보보호관리시스템의 관리범위 설정이 편리해지고, 부별 역할 및 책임

정의와 그에 따른 업무표준화 작업이 가능해 진다.

둘째, 정보보호 수준진단 측정 모델을 통해 기존 평가표 형식의 문제점(문서화 집중이나 문서량 증가, 실질적인 보안통제 관리방법의 부족 등)을 해결할 수 있다.

셋째, 주요 개선사항(보안지표 점수 저조항목)에 핵심적인 역량을 집중하도록 업무체계를 개선하며, 시스템 고도화를 통해 보안위협의 조기경보(위험관리)와 정보보호 포털을 위한 연계환경 구축이 가능해 진다.

본 측정모델은 기존 모델과 대비해 볼 때, 정성적이고 편향적인 IT 중심의 기술보안 관점에서 벗어나 다양한 관리지표 POOL을 활용하여 각 기업의 특성에 맞는 객관적이고 종합적인 정보보호 수준 진단 및 평가체제 구축을 통하여, 보다 더 개관적이고 분석적인 방법으로 정보보호의 취약부문을 사전에 탐지하여 보안사고를 예방할 수 있는 효과를 거둘 수 있도록 설계되었다.

V. 결 론

지금까지 살펴본 내용을 간략히 요약해 보면, 본 연구 논문에서는 각 기업체에서 겪고 있는 다양한 형태의 보안사고 위험을 줄이기 위한 측정 도구로써, 객관적이고 실질적으로 적용할 수 있는 정보보호수준 측정 모델 및 관리기준을 정립하였다.

즉, 국내외 선진기업에서 사용 중인 보안수준 진단 및 측정모델의 사례와 ISO27001을 기반으로 한 평가모델을 바탕으로 종합적인 지표 POOL을 작성하여 측정모델을 설계한 후, 수차례 테스트와 Data의 신뢰성 검증 등을 통하여 각 기업에서 범용적으로 활용할 수 있는 수준까지 개선을 하였다.

그러나, 본 연구에서 소개된 측정모델 역시 부분적인 한계점을 지니고 있기 때문에 보다 실용적이고 합리적인 모델로 발전하기 위해서는 지속적인 활용과 함께 보완작업을 거쳐야 한다고 본다.

특히 본 모델이 각 기업에 적용되기 전에 우선적으로 검토해야 할 사항들은 측정모델의 적용 편리성과 평가결과에 대한 각 현업부서의 수용성, 그리고 평가항목 선정의 적정성 및 평가자(평가 주관부서)와 피 평가자(피평가부서) 간의 평가기준에 대한 명확한 이해 등이다.

또한 측정모델을 지속적으로 유지/발전시키기 위한 데이터의 축적 및 활용도 제고 노력이 필요하며, 최근 정보보호 활동에 있어서 가장 큰 이슈가 되고 있는 인적 보안의 취약점을 비롯한 핵심적인 관리 포인트(첨단기술 및 기밀정보 보호활동, 핵심인력 및 가치 있는 정보자산의 관리 프로세스 정립 등)를 선별하여 적절한 가중치를 부여한 후, 선택과 집중형태의 정보보호 관리체제를 강화해 나가야 한다는 점이다.

향후에도 본 측정모델을 각 기업에 실제 적용하면서 지속적인 유지 및 보완작업을 해 나감으로써, 보다 실용적이고 정교한 정보보호수준 측정 도구로 활용될 수 있도록 개선되었으면 한다.

참고문헌

[1] 한국정보보호진흥원, 2007 정보시스템 해킹·바이러스 현황 및 대응, *한국정보보호진흥원* 2007

[2] 첨단 산업기술 보호동향 (8호), 2007. 9 *국가정보원*

[3] ISO/IEC27001 : 2005(FDIS) Information Security Management System Requirements

[4] 최선태, 기업보안 관리전략, *인포더* 2008

[5] concert, 2008 Security Forecast 발표자료, 2008. 3

[6] Robert S. Kaplan & David P. Norton, 전사적 전략경영(SEM)을 위한 SFO, *한언* 2001. 8

[7] Robert S. Kaplan et. al., 가치실현을 위한 통합경영지표 BSC, *한언* 2007. 6

[8] SP800-53(Rev.2) : Recommended Security contorls for Federal Information Security, 2007. 10 *NIST*

[9] ISO/IEC 27004(Draft) Information Security Management measurement

[10] SP800-55 : Security Metrics Gudie for Information Technology Systems 2003, *NIST*

[11] ISO/IEC 27002(FDIS) The Code of Practice for Inforamtion Security Management

〈著者紹介〉

이 희 명 (Hee-Myung Lee) 정회원
1984년 2월 : 충남대학교 경영학과 경영학사
2006년 9월~현재 : 고려대학교 정보경영공학전문대학원 석사과정 (정보보호전공)
1984년 2월~현재 : 포스코 (정보보호그룹장)
<관심분야> 정보보호정책, 프라이버시보호, 산업보안

임 종 인 (Jongin Lim) 종신회원
1986년 2월 : 고려대학교 대학원 수학과 박사(암호학)
2000년 8월 : 고려대학교 정보보호대학원/CIST 원장(센터장)
2004년 1월 : 국가정보원 정보보호정책 자문위원
2005년 7월 : 대통령 자문 전자정부 특별위원
2005년 12월 : 국회 과기정위원회 정보통신 정책 자문위원
<관심분야> 정보보호기술, 정보보호정책, PET, 컴퓨터 포렌식