情 報 保 護 學 會 誌
第20卷 第1號, 2010. 2

기업 정보보호 이슈 및 방향

김 인 호*, 이 기 혁**, 박 종 희***

요 약

최근 정보기술의 발달로 해킹 등 각종 보안위협이 증가하고 있으며 이는 기업 경영에 심각한 위협으로 다가오고 있다. 해킹을 당한 기업은 금전적인 손실과 더불어 기업 이미지에 심각한 타격을 입고 뒤늦게 정보보호의 중요성을 인식하여 보안 대책을 수립하고 있지만 주먹구구식인 경우가 대부분이다. 본 논문에서는 기업의 중요자산과 정보시스템을 보호하기 위해 반드시 고려해야 할 보안관리 방안을 제시하고 SK텔레콤의 사례를 설명하려 한다.

Ⅰ. 서 론

최근 정보기술의 발달로 해킹 등 각종 보안위협이 증가하고 있으며 이는 기업 경영에 심각한 위협으로 다가오고 있다. 과거의 해킹은 해커 자신의 실력을 과시하기 위해 행해 졌으나 최근의 해킹은 실력과시 보다 금전적인 이득을 취하거나 정치적인 목적의 해킹이 늘고 있다. 개인정보유출, 게임 아이템 해킹, 금융거래 해킹이 빈발하고 있으며 개인정보유출 및 금전적 손해를 입은 피해자들이 기업을 상대로 집단 소송을 하는 등 사이버 보안 사고로 인해 기업들은 생존의 위협을 받고 있다. 해킹 뿐 아니라 네트워크가 감당하기 어려울 정도의 대규모 접속신호를 여러 대의 PC에서 보내 사이트를 마비시키는 분산서비스거부공격(DDoS)를 통해 사이트를 마비시키고 이를 풀어 주겠다며 돈을 뜯어내는 협박도 기승을 부리고 있다. 기업의 정보 시스템이 마비되거나 파괴될 경우, 해당 기업의 주요 업무도 당연히 마비될 수밖에 없다. 이는 동시에 EH 다른 해커의 목표가 될 수 있으며, 직접적인 매출 감소와 고객 이탈, 신규 사업 제한, 기업의 브랜드 이미지 가치 추락을 면하기가 어렵다. 이런 이유로 기업들은 정보보호의 중요성을 인식하고 보안 대책을 수립하고 있지만 일회성이고 주먹구구식인 경우가 많다.

2008 정보보호실태조사 결과를 살펴보면 국내기업들의 침해사고 대응현황은 60% 이상이 '보안과 관련해 별다른 대응활동을 하지 않는다'고 파악돼 해킹을 당하고도 사후조치를 취하지 않는 것으로 나타났다[1]. 또한 73%이상은 '재해나 침해사고에 대비해 비상복구 계획이 없다'로 답해 기업이 자산에 대한 관리를 제대로 수행하고 있지 않아 항상 위험에 노출 되어 있는 것으로 조사됐다. 정보보호를 위한 투자를 보면 국내기업은 75%가 IT투자 대비 1%미만을 정보보호에 투자하고 있다. 반면 미국과 영국은 10% 기업만 IT투자 대비 1% 미만을 차지해 우리나라와는 커다란 차이를 보이고 있다. 기업이 정보보호활동을 비용이 아닌 투자활동으로 생각하고 적극적인 노력을 기울여야 자산을 보호할 수 있지만 현실은 그렇지 못하다.

따라서 본 논문은 기업 자산에 대한 정보보호의 필요성을 인식시키며, 효과적인 정보보호를 위해 필요한 관리 방안을 제시하고 SK텔레콤의 사례를 설명하려 한다.

Ⅱ. 기업 정보보호 활동 현황

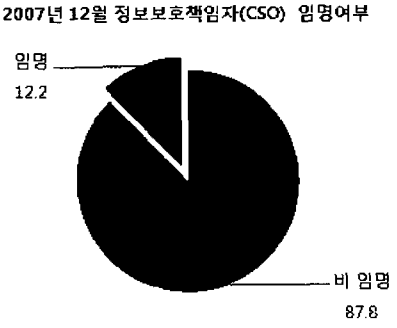
2.1 최고보안책임자(CSO) 선임

CSO(Chief Security Officer)란 전사적 차원에서 정보시스템은 물론 인적, 물적 보안체계를 안전하게 관리하고, 운영과 통제를 책임지는 최고위직 임원이다.

* SK텔레콤 IT보안팀 (ino1170@sktelecom.com)
** SK텔레콤 IT보안팀장 (kevinlee@sktelecom.com)
*** SK텔레콤 IT보안팀 (falcon@sktelecom.com)

기업에서의 CSO의 역할은 기업의 비전과 경영상황, 사업 분야에 대한 고찰을 통해 전사 차원의 정보보호 정책과 운영절차를 결정하는 한편, 정보시스템을 비롯한 주요 업무에 대하여 취약성 분석과 위험 분석을 상시·비상시 실시하여 적정한 위험수준을 유지하도록 하는 것이다[6]. 또 해킹이나 바이러스 등에 대응하기 위해 자사의 IT인프라에 적합하고 투자대비효과(ROI)측면에서 적정한 정보보호 솔루션을 도입하여 기업 내·외부의 악의적 공격에 대응 가능한 모습을 갖추는 것도 CSO가 담당해야 할 역할이다. 이러한 역할은 기업의 경영활동 내용과 기업이 속한 산업 군에 따라 변화하기도 하는데, 정보시스템을 중심으로 한 소프트웨어나 인터넷 비즈니스 기업은 애플리케이션과 데이터에 대한 정보보호 체계의 운영 및 유지가 일차적인 과제가 되지만, 기존의 정형적 기업체계에서는 출입통제를 비롯한 물리적 보안시스템의 운영이 중시된다. 하지만 정보시스템의 역할이 확장됨에 따라 어느 한쪽만을 선택할 수 있는 것은 아니다.

CSO의 선임은 기업에 있어서 기술적 이슈라기보다는 문화적인 측면과 경제적인 측면이 고려된 비즈니스 이슈로 다뤄져야 한다. 정보보호는 경영을 위한 일개 요소라기보다는 경영 전체를 위한 인프라라고 봐야 한다. 기업이 안정적으로 사업을 영위하면서 대외적으로 신뢰를 구축하기 위해서는 완벽에 가까운 정보보호체계의 수립이 요구되며, CSO는 이러한 활동의 최전방에 위치하고 있다. SK텔레콤에서는 CSO임원을 선임하여 전사 정보보안 전략방향을 정립하고 정기 미팅, 사고대응 프로세스, 이슈관리 프로세스 등 전사보안운영체계를 수립하여 전사정보보안회의를 통해 임원, 팀장, 실무자가 참여하여 많은 의견을 나누고 있다.



〔그림 1〕 정보보호책임자 임명 여부 (단위 : %)

2.2 정보보안 인프라 투자

현대 사회의 IT환경은 하루가 다르게 변하고 있다. 모든 생활이나 의식주가 정보화를 배제하고는 이제는 생각조차 할 수 없는 시대에 우리는 살고 있다. 기업의 업무 환경도 빠르게 변화하여 인터넷을 이용해 재택근무를 하거나 이동 중 스마트폰으로 이메일을 확인하고 회의실로 이동해서 회의를 할 때는 무선 랜을 이용하여 사내 전산망에 접속한다. 이러한 새로운 환경에서는 새로운 정보보안 문제가 반드시 존재한다. 새로운 정보보안문제는 기존에 구축되어진 정보보안 인프라를 가지고 예방 및 방어할 수 없다. 결국 정보보안 인프라에 대한 투자가 적극적으로 이루어져야 해결 할 수 있다. 하지만 우리는 정보보안에 대한 투자가 인색한 것이 사실이다.

최근에 와서 정보보안에 대한 인식이 조금씩 바뀌고 있고 투자가 발생하는 것은 사실이나 지속적이고 장기적인 투자가 아니라 일회성 투자라는 측면이 선진국과 비교된다. 또한 2008년 한국정보보호진흥원 정보보호 실태조사에서 기업에서 '정보보호 지출 없음'이 44.5%로 정보보호에 대한 투자가 저조한 것을 볼 수 있다. 선진국들은 정보보안을 인프라 측면에서 이미 수많은 투자를 해 왔으며 그만큼 IT환경의 보안대책이 어느 정도 안정화를 가져온 상태에서 지속적으로 투자를 하고 있다. SK텔레콤은 새로운 위협에 대응하기 위해 무선침입방지시스템 및 DDoS 차단 시스템을 신규로 도입하여 새로운 위협에 대응하고 있으며 신규 비즈니스에 대한 사전 보안취약점 점검 및 취약점 제거를 통해 보안위협을 사전에 방지하고 있다. 또한 프로그램 개발 시 개발자에 대한 보안 취약점 제거를 위해서 소스코드에 대한 점검을 강화하여 개발단계부터 개발보안 프로세스를 개선함으로써 취약점을 원천적으로 제거하는 환경을 구축하여 운영하고 있다.

〔표 1〕 정보화 투자 대비 정보보호 투자 비율 (단위: %)

내용	2007년	2008년
정보보호 지출 없음	50.8	44.5
1% 미만	27.5	22.2
1%~3% 미만	11.4	15.3
3%~5% 미만	5.1	8.2
5%~7% 미만	1.8	3.4
7%~10% 미만	2.3	6.0
10% 이상	0.8	0.3

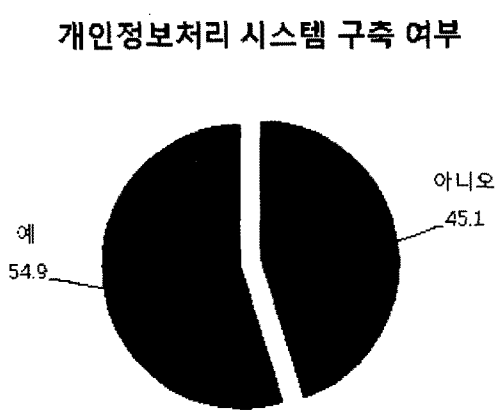
기업 내부의 IT인프라는 시스템·네트워크·전산센터 뿐만 아니라, 정보보안에 대한 투자도 이제는 인프라로 인식하게 될 때 기업은 정보보안문제로부터 조금씩 안전하게 개선될 수 있을 것이다. 정보보안에 대한 투자를 비용으로 인식하는 기업 경영진들이 있을 때, 기업은 여전히 정보보안문제에 노출 될 수밖에 없다. 기업은 정보보안에 대한 투자의 시선을 긍정적으로 바라볼 필요성이 있다. 정보보안에 대한 투자로 인해 기업의 정보가 안전하게 관리된다면 국제적인 경쟁에서 대외 신인도 향상 및 고객의 신뢰성을 확보하는 기대 이상의 효과를 볼 수 있는 결과를 가져오게 될 것이다. 또한 매년 수행하는 보안취약점 진단 및 평가 또는 모의해킹 등을 자칫 잘못 인식할 경우 매년 똑같은 일을 되풀이 하는 것이 아닌가? 지적하고 오해할 수 있으나 이는 시시각각으로 변화하는 IT환경과 새로운 정보화 환경으로서의 패러다임 변화, 다양한 해킹 패턴의 변화 및 변종 바이러스의 발생 등을 인지하지 못한 것이라 볼 수 있으며 이에 대응하기 위해서는 1년에 한 번씩 수행할 것이 아니라 주기를 더욱 단축해야만 새로운 환경의 변화에 적응할 수 있는 정보보안 대책을 마련할 수 있을 것이다.

〔표 2〕 정보보호 지출이 없는 이유 (단위 : %)

내용	2007년	2008년
필요성을 못 느낌	50.1	41.2
관심 없음	15.2	24.3
방법을 모름	4.0	15.2
예산 없음	7.8	12.3
이미 충분히 투자	3.0	3.2
기타	4.2	3.8

2.3 고객 정보보호

기업이 확보하고 있는 고객의 개인정보는 기업의 기술정보와 같이 미래의 경제적 이익을 가져다주는 핵심자산이다. 마케팅에서 기업은 고객을 일회성 구매능력이 아니라 평생에 걸쳐 거래기업에 대해 제공할 수 있는 잠재적 공헌도로 평가하고 있다. 고객정보는 다른 무형자산과 달리 기업이 창조한 것이 아닌 고객으로부터 빌려 온 자산이다. 자본을 투자한 주주에게 수탁관리의 책임이 있고 부채를 빌려준 채권자에게 이자와 원금상환의 의무가 있듯이, 기업은 개인정보를 제공한 고객에



〔그림 2〕 개인정보처리 시스템 구축 여부 (단위 : %)

게 개인정보의 성실한 관리라는 빚을 지고 있다고 기업은 인식해야 한다. 기업의 고객정보보호는 단순히 규제대응을 하지 못해서 발생하는 위험을 예방하는 차원의 활동 그 이상의 것이다.

최근 국·내외 적으로 인터넷 및 전사상거래의 활용이 급속히 확산되면서 인터넷 서비스업체에 제공된 개인정보가 범죄에 사용되는 등 무분별한 개인정보 수집·이용이 급증하고 있다. 또한 해킹에 의해 기업들이 소유하고 있는 고객정보가 유출되어 고객들이 기업을 상대로 집단소송을 하는 등 기업의 고객정보보호가 국민들의 깊은 관심을 받고 있다. 그러나 아직도 전자상거래 사업자 등 다양한 분야에서 고객정보 관리자들은 날로 그 가치를 더해가고 있는 고객정보를 이용하여 가능한 한 더 많은 이윤을 남기기 위하여 정보주체가 모르는 사이에 수집, 프로파일링 또는 제3자에게 매매하는 등 개인정보 침해의 주된 원인을 제공하고 있다.

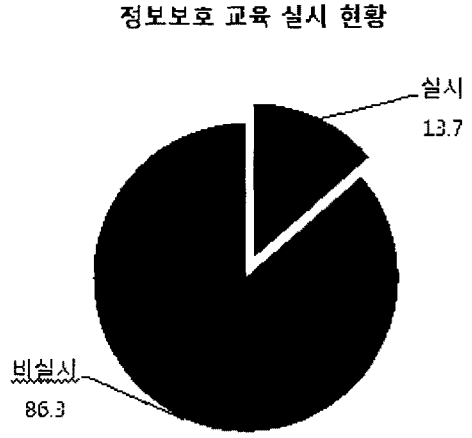
개인정보 유출사고는 매우 다양한 경로를 통하여 발생 할 수 있다[4]. 개인정보가 생성, 처리, 저장, 활용되는 기업 내 시스템에서 정보가 전달되는 네트워크상에 이르기까지 개인정보로의 접근이 가능한 모든 곳이 유출 경로가 될 수가 있는 것이다. 기업 내 고객정보 유출은 말 그대로 기업 내 축적된 고객정보가 외부로 유출된 경우로 포털사이트나 인터넷 쇼핑몰, 통신업체, 은행 등에서 관리 소홀 또는 의도적으로 고객정보를 유출한 사례를 언론을 통해서 심심치 않게 볼 수 있다. 그리고 개인정보처리를 전문적으로 하는 시스템을 구축한 곳도 45.1%로 전체 절반도 못 미친다. 기업은 기업 내 보관되고 있는 고객정보에 대한 보다 철저한 보안관리 대책

이 필요하며 그에 대한 기술적인 대응 방안으로는 데이터베이스에 저장된 고객정보를 보호하기 위한 DB보안 솔루션 도입 및 내부자에 의한 고객정보로의 부적절한 접근을 방지하기 위한 시스템과 체계를 구축할 필요가 있다. SK텔레콤은 고객정보전송시스템을 구축하여 고객정보 전송 시 정보유출 가능성을 감소 시켰고, 고객정보를 암호화하여 유출시 피해를 최소화 시켰다.

2.4 내부 정보보호

최근 신문지상에는 다양한 정보 유출 사건들이 보도화되고 있다. 국정원에서는 조선 기술을 유출시키려던 전직 조선업체 직원을 검거했다는 보도와 함께 유출하려던 조선 기술과 설계도면은 그 동안 투자한 연구 및 개발 비용만 5000억 원이며, 만약 이 기술이 유출되었다면 중국 업체는 앞으로 5년간 최소 35조원 규모의 수주를 할 수 있는 정도로 중국이라는 나라의 인건비를 감안한다면 국내 조선업계가 통째로 경쟁력 저하로 피해를 입을 수 있었을 만한 사건이다.

검찰이 적발한 A사의 휴대인터넷 기술유출 사건은 기술을 개발해놓고도 누구나 열람할 수 있도록 방치하는 등의 보안관리가 허술하여 15조원에 달하는 천문학적인 손실을 입을 뻔 했다. 남의 이야기처럼 들리는 이와 같은 사건 사고는 단순히 신기술을 개발하거나 고부가가치 산업에서만 발생하는 것이 아니다. 2007년 초 조사에 따르면 국내 기업의 20% 정도의 기업에서 중요 기밀이 유출돼 피해를 본 적이 있고 피해기업의 기밀유출 횟수도 평균 3회에 달하는 등 피해가 심각한 것으로 나타났다. 오랜 시간 투자를 통해 이뤄낸 연구의 성과나 기술자료, 도면이나 소스코드와 같이 유출 시 기업의 투자비용 회수나 재투자가 어려운 정보 유출의 경우 기업의 생존, 나아가 국가 전체의 산업 기반에도 영향을 미칠 수가 있다. 기업의 중요 정보에 대한 유출경로는 외부의 침입으로 인한 정보유출보다는 기업 내부자에 의한 정보유출이 훨씬 높은 비중을 차지하고 기밀정보의 접근 용이성으로 그 피해액도 내부자를 통한 유출이 훨씬 더 큰 경제적 손실을 주게 된다[7]. 하여 내부의 지적자산 보호를 위한 근본적인 보안대책 마련이 시급하게 요구되고 있다. SK텔레콤은 네트워크 접근제어 환경을 구축하여 외부자에 의한 내부 네트워크 침입을 최소화 했으며 모든 문서에 문서보안을 적용하여 외부유출시



[그림 3] 정보보호 교육 실시 현황 (단위 : %)

피해를 최소화 하도록 하고 있다.

기업의 안전한 정보보호 환경을 위해 기업은 보호할 대상을 명확히 해야 한다. 가장 중요한 정보가 무엇이며 보호되어야 할 정보는 무엇인지, 그것이 어느 정도의 가치를 가지고 있는지 그리고 정보는 조직 내에서 어떻게 존재하고 있는지 이런 것들을 명확히 정의하고 보호할 방안을 세워야 한다.

보호가 필요하다고 정의된 정보는 정확한 업무 흐름에 대한 파악을 통해 보호할 대상의 접근방식에 대한 전략을 세워야 한다. 정보를 보호하기 위해서는 적절한 대응 방안이 필요함으로 보호 대상 정보가 조직 내에서 어떠한 식으로 생성, 저장, 사용, 전송, 폐기되는지 즉 라이프사이클이 어떻게 되는지 또 그것이 업무 속에서 어떻게 취급되고 있는지를 알아야만 해당 라이프사이클 또는 취급상에서 정보가 유출될 수 있는지 파악할 수 있을 것이다. 또한 인적 보안은 성공적인 보안 관리 수립에 필수적인 항목으로 내부 정보를 실질적으로 사용하는 사람에 대한 관리 방안이나 적절한 통제 방안을 제시해야 한다. 정보를 다루는 것도 정보를 유출하는 것도 역시 사람으로부터 발생하는 것으로 모든 정보 보호 방안의 중점은 사람이 우선시 되어야 한다. 그러나 인적 보안은 교육만으로 해결할 수 없다.

시스템을 통해 내부 사용자와 악의적인 외부 침입자들을 통한 정보 유출 가능성을 배제하고 강력한 보안 정책을 통해 내부 사용자들을 통제하고 보안 의식을 고취 시켜야 할 것이다.

2.5 침해사고대응팀(CERT) 운영

네트워크 인프라와 기술이 계속적으로 발전되고 있는 환경 속에서 국내·외 보안 침해사고가 점점 지능화, 다양화, 대중화되고 잇다. 보안 위협이 속출하는 현실 속에서 기업 네트워크에 대한 침해사고가 발생하였을 경우 신속한 침해사고 대응이 필요하다. 침해사고대응팀은 조직 내의 침해사고를 예방하고 복구하는 업무를 수행하는 팀으로 조직의 전산망에 발생하는 침해사고 대응활동을 주관하고 지원하는 업무를 수행하는 정보보호 조직이다[5]. 침해사고대응팀의 목적은 조직의 정보자산을 안전하게 보호하는 것이다.

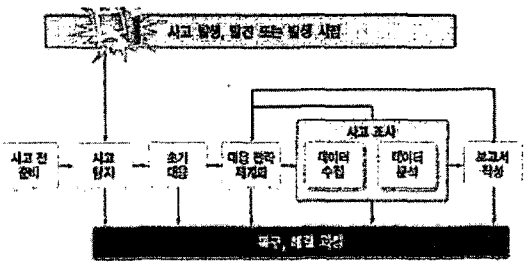
국내기업의 침해사고 대응 활동에 대해 살펴보면 별다른 활동을 하지 않는 기업이 2008년 기준으로 61.1%, 침해사고대응팀을 구축/운영하는 기업은 9.6%인 것으로 나타나 기업들의 침해사고 대응에 대한 관심과 노력이 필요한 것을 알 수 있다. SK텔레콤은 Information Security Service Watch(ISS-W) 시스템을 구축하여 신속한 침해사고대응 활동을 하고 있다.

〔표 3〕 정보보안 침해사고 대응 활동 (단위 : %)

비율	2007년	2008년
긴급연락 체계 구축	20.2%	14.8%
침해사고 대응 계획 수립	15.2%	13.9%
외부 전문기관 위탁	13.6%	12.4%
사고복구조직 구성	9.6%	8.7%
CERT구축/운영	5.6%	9.6%
별다른 활동 하지 않음	61.9%	61.1%
기타	20.	4.4%

침해사고 대응절차는 실제 발생한 침해사고를 체계적인 방법으로 신속하게 대응할 수 있는 핵심 사항이다. 침해사고 대응절차를 효과적으로 구현하기 위해서는 조직의 정보보호 규정으로 선언하는 것이 중요하다. 규정화 되지 않는 경우 각 담당조직 간의 역할과 책임이 불분명하여 효과적인 침해사고 대응을 어렵게 할 수 있기 때문이다.

국내에서는 참고할 만한 사례로 한국정보보호진흥원의 침해사고 대응절차가 있다. 총 7단계로 구성돼 있으며 사고 전 준비→사고탐지→초기대응→대응 전략 체계화→데이터수집→데이터 분석→보고서 작성으로 완료된다[3]. 각 기업은 조직 구성과 정보보호 규정에 맞는 침해사고 대응 절차를 설계해야 한다.



〔그림 4〕 한국정보보호진흥원 침해사고 단계별 처리 절차

Ⅲ. 결 론

기업의 성공적인 정보보호를 위해서 기업은 종합적이고 장기적인 접근을 하도록 해야 한다. 로마가 하루아침에 이루어지지 않았듯이 기업의 보안도 현재 상황을 파악하여 미래지향적인 사고로 일관되고 실용성 있게 추진해야 할 것이다. CSO를 중심으로 전사적인 정보보안체계를 구축하고 정보보안 마스터플랜과 같은 중장기적 관점에서 정보보안 강화를 위한 방향과 전략, 과제를 도출함으로써 다양한 보안 위협으로부터 지속적으로 비즈니스를 안전하게 보호하기 위한 기반을 조성해야 한다. 또한 고객정보보호는 아무리 강조해도 지나치지 않다. 고객정보보호를 강화하기 위해서 별도의 물리적인 환경을 구축하고 개발자 등 고객정보를 다량으로 취급하는 사람들은 보안 모니터링을 강화할 필요가 있다. 고객정보를 외부로 보낼 때는 법적 규제사항을 준수하기 위해 별도의 암호화된 채널을 통해서만 송수신할 수 있는 프로세스와 시스템을 구축하는 방법을 고려해 볼 수 있다. 마지막으로 내부정보보호 강화를 위해 기업의 기밀정보가 외부로 유통되는 경로를 모니터링 하여 관리할 수 있는 체계를 마련하고 퇴직자와 관련된 프로세스를 개선하여 내부정보 유출을 관리해야 할 것이다.

보안은 사슬과 같아서 가장 약한 고리만큼만 안전하고, 보안은 기술이 아닌 일련의 과정이다[2]. 하여 현재 내 기업의 가장 약한 고리를 찾아서 강화하고 과정을 만들기 시작해야 할 것이다.

참고문헌

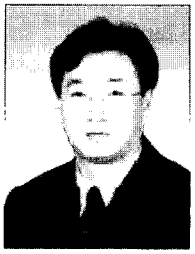
[1] 한국정보보호진흥원, "2008 정보보안실태조사",

2008. 11.
[2] 브루스 슈나이어, "디지털 보안의 거짓말", 나노미디어, pp. 10-11, April 2001.
[3] 한국정보보호진흥원, "침해사고 분석 절차 가이드", 2007. 9.
[4] 김정덕, "개인정보보호를 위한 관리체계와 거버넌스", 정보보호학회지, 18권, 6호, pp. 1-5, 2008.
[5] 한국침해사고대응팀협의회 · 한국정보보호진흥원, "CERT 구축 및 운영 가이드", 2007. 9
[6] 정보보호실천협의회, "기업 정보보호 실천 가이드 2007, 월간 정보보호21c, 2007.
[7] 조재형, "내부 정보보호를 위한 전략 수립 방안", Network Security Fair 2006, 2006.

〈著者紹介〉

김 인 호 (Kim, In-ho)
2004년 2월: KAIST 테크노경영대학원 석사
2006년 2월: 한국정보보호진흥원 선임연구원
2008년 8월: SK텔레콤 정보기술원 IT보안팀 매니저
<관심분야> 정보보호

이 기 혁 (Lee, Gi-Hyouk)
정회원
1990년 2월: 한양대학교 공학석사
1997년 3월: 한국이동통신(주) 정보기술연구원 N/W 운용팀장
2001년 8월: SK텔레콤 플랫폼연구원 IT 인프라개발팀장
2008년 1월: SK텔레콤 IT 보안팀장
<관심분야> 전자공학, 통신공학, 정보보호



박 종 희 (Park. Jong-Hee)
1996년 2월: 중앙대학교 경영정보학사
2002년 11월: SK텔레콤 정보기술원 IT보안팀 매니저
<관심분야> 정보보호