http://dx.doi.org/10.14400/JDPM.2013.11.11.305

신정보화 환경에서 중소기업 기술유출에 대한 인식과 관리 실태에 관한 연구

김기호*, 하규수**
중소기업기술정보진흥원 경영정보화부 부장*, 호서대학교 벤처전문대학원 벤처경영학과 교수**

The Research on Security Cognition and Management Status of Technology Outflow about Small-medium Companies in New IT Environment

Kim, Ki Ho*, Ha, Kyu Soo**
Korea Technology and Information Promotion Agency for SMEs*
The Graduate School of Venture, Hoseo University**

요 약 이 연구의 목적은 신정보화환경에서의 중소기업의 기술유출에 대한 보안인식 및 보안관리 실태를 측정하고, 대기업과 중소기업간의 수준비교분석을 통해 기술유출 방지대책을 위한 정책의 기초자료를 제시하고자 한다. 분석결과 보안인식 및 보안관리실태 모두 중소기업은 대기업에 비해 열악한 것으로 나타났으며, 정보화환경의 급격한 발달에 따른 부문별 관리가 필요한 상황인 것으로 보인다. 현재 중소기업의 신정보화환경 구축은 도입기에 있으므로, 구축과 동시에 보안시스템을 함께 갖출 수 있는 지원이 필요하며, 동시에 중소기업 자체적 대응이 가능하도록 신정보화환경에 맞는 보안시스템이 필요하다. 중소기업의 경우 급변하는 정보화환경의 변화에 따른 기술보호 역량을 갖추기에는 한계가 있음으로 정부의 체계적인 보안관리 지원이 요구된다.

주제어 : 신정보화, 기술유출, 중소기업, 정보보안, 보안인식, 보안관리

Abstract This research suggests the security countermeasures for solving technology outflow of small-medium companies in New IT Environment through level comparison of security cognition and security management between small-medium companies and major big companies. According to analysis results, it is poor for small-medium companies' level of security cognition and security management compared with major big companies. Small-medium companies need to manage technology outflow to major big companies' level in New IT Environment. Small-medium companies has started to build New IT Environment recently and it must build the appropriate security system for small-medium companies at the same time. Small-medium company has more problem with budget and proffessionals to maintain the security of technology outflow. Therefore government has to support systematic management for the security of technology outflow to Small-medium companies

Key Words : New IT Environment, technology outflow, small-medium company, technology security, security cognition, security countermeasure

Received 30 October 2013, Revised 20 November 2013
Accepted 20 November 2013
Corresponding Author: Ha, Kyu-Soo (The Graduate School of Venture, Hoseo University)
Email: ksh@hoseo.edu

ISSN: 1738-1916

1. 서론

1.1 연구의 필요성

최근 급변하는 신정보화 환경으로 인하여 정보보안 시스템의 복잡도가 증가되고 있다. 기업의 각종 활동이 스마트폰, 태블릿PC등 신정보화 기기에 연결된 정보통신망에서 이뤄지고 있으며, 이러한 사무기기 및 정보통신의 발달은 정보의 유출을 용이하게 만들고 있어 새로운 환경에 맞는 적절한 통제가 필요하게 되었다. 본 연구에서는 신정보화환경을 모바일 환경의 확산과 정보통신 인프라 확충에 따라 기업이 스마트폰이나 태블릿PC등의 새로운 정보화 기기를 이용하여 모바일 오피스와 클라우드 서비스 등을 업무에 활용하고 있는 환경으로 정의하였다.

신정보화 환경에서는 각 디바이스를 통해서 어느 곳에서나 정보의 이동이 용이하다. 이것은 어디에서든지 정보가 유출될 수 있음을 의미한다. 이에 따라 신정보화 기술의 발달에 따른 기술유출의 수단이 유체물에서 무체물인 이메일, 디지털 자료 복사 등으로 첨단화되고, 범죄 수법이 지능화 되어 가고 있는 실정이며, 이와 같은 신정보화 환경에서의 보안 문제는 기존의 기술유출 관리에서는 경험하지 못했던 새로운 문제가 부각되고 있으며, 신정보화 기기로 인해 보안위협 및 취약성이 증가하여 침해사고 발생 가능성이 높아지고 있다. 특히 스마트폰을 포함한 와이브로 서비스 등을 이용하는 신정보화 환경에서는 기존 정보보안시스템 기능으로는 완벽한 차단을 기대하기 어려우며, 기술 정보 유출에 대한 감시 및 보안체계는 상대적으로 취약해질 수 밖에 없다.

이와같이 신정보화 환경에서 업무가 이루어지는 빈도가 높아질수록 조직 내·외부로부터의 정보유출 위협요소가 증가하고 있으나 기업의 기술정보를 효과적으로 관리하고 통제하기 위한 기술유출 대응은 취약하다. 신정보화 환경에서는 기술유출 방지에 대한 목표를 효과적으로 달성하기 위해서 조직수준(Managerial Level)의 관점에서 일관성 있는 정보보호 체계 구축이 필수적이며, 위험을 예측하고 이를 예방하기 위해서는 물리적, 기술적 수단 외에 관리적 수단도 동원되어야 한다. 특히 중소기업은 대기업과 달리 신정보화 환경에서의 기술보호의 위협이나 기술유출의 가능성에 대한 인식이 부족하며, 예산 부족 및 전문 인력 부족으로 적절한 대응이 이루어지지 못하고 있는 실정이다.

1.2 연구 목적

본 연구에서는 중소기업의 신정보화환경에 대한 기술유출 대응실태의 분석을 통해서 신정보화환경에서 적절한 기술보호대책을 수립/적용함으로써 기술보호의 실효성과 기술유출을 예방할 수 있는 방안을 제시하여 기술유출방지시스템 구축사업을 위한 정책의 기초자료로 활용하고자 한다.

신정보화 환경에서의 기술유출의 가능성과 기술유출 취약점을 도출하고, 신정보화 환경의 기술적, 관리적 위협요소와 취약점에 대한 대책을 제시하였다.

정부에서 시행중인 중소기업 신정보화 지원사업은 중소기업의 업무 효율성 향상을 위해 기존의 사내 정보시스템을 모바일 서버에 연동하여 모바일 기기로 구현할 수 있는 무선네트워크 환경 및 시스템 개발을 지원(모바일 오피스 구축 지원사업)하고, 초기 투자비용 없이 중소기업이 활용할 수 있는 클라우드 기반의 모듈별 정보시스템을 제공하고 시스템 구축 및 관리는 위탁운영하도록 지원(클라우드형 정보화 지원사업)하고 있다.

신정보화 지원과 함께 이에 최적화된 기술유출방지대책이 지원초기부터 이루어져야 할 필요가 있다는 관점에서 중소기업의 신정보화 환경 구축실태 및 업무활용도를 조사하고, 신정보화 환경에 대한 보안인식 및 보안관리 실태를 분석하여 신정보화 환경에서의 기술유출 방지대책에 대한 정책방향을 제시하고자 한다.

2. 이론적 배경

본 연구에서는 신정보화환경에서 발생할 수 있는 기술유출 위협요인을 분석하기 위해 새로운 IT인프라가 적용된 신정보화 환경에서의 정보보호 관련 연구를 토대로 기술유출의 위협요인을 기술적부문과 관리적 부문으로 나누어 분석하고자 한다.

2.1 기술적 부문의 위협요인

기술적 부문의 위협요인에 관한 내용을 선행연구를 통해 살펴보면, 이형찬(2011)은 휴대기기의 특성상 사용기기의 분실 및 도난, 사용자인증문제가 보안위협의 주

요요인이 된다고 밝혔고, 보안대책으로 단말인증 및 원격제어대책등을 제시했다[2]. 임종인(2011)은 사용자기기부문의 위협요인으로 스마트폰 단말 분실 및 도난을 제시하였고, 이에 대한 문제점 해결 방안으로 MDM (Mobile Device Management)[1]솔루션을 통한 파일배포, 원격 잠금 설정, 원격 데이터삭제 등의 보안기술적용을 제시했고, 네트워크 환경부문에 대한 기본적인 대책으로 망 분리를 제시했고, 내부 망 보호를 위한 접속제한 및 접속 차단을 위한 중앙제어가 필요하다고 했다[4]. 나종회(2012)는 스마트워크 환경에서의 보안 위협을 단말, 소프트웨어/플랫폼, 네트워크 등 3가지 스마트워크 서비스 계층 관점에서 최종적으로 16가지의 스마트워크 보안 위협을 제시하였다[3]. 장은영(2011)는 모바일 클라우드 서비스 환경에서의 위협요인을 모바일기기, 무선네트워크, 클라우드서비스 세가지 관점에서 분석하였고, 이기주(2013)은 스마트 사회의 보안위협을 스마트폰 보안위협, 소셜네트워킹환경의 보안위협, 클라우드서비스의 보안위협, 빅데이터 환경의 보안위협으로 분류하여 분석하였다.[1],[7]. 이경복(2011)은 새로운 정보화 환경에서의 보안위협을 기술적인 측면에서 스마트폰 플랫폼, 애플리케이션, 네트워크에서 주로 발생한다고 분석하였다. 나종회(2012)는 기존의 선행연구들을 바탕으로 탐색적 연구를 통해 제시한 16가지의 스마트워크 보안 위협을 단말, 소프트웨어/플랫폼, 네트워크의 3가지 관점에서 분류하였다[3].

기존의 선행연구들은 스마트워크환경, 클라우드서비스환경에서의 정보보호에 관한 연구들이다. 본 연구에서 규정한 신정보화 환경은 이러한 모든 새로운 IT인프라가 적용된 환경을 지칭하는 것이므로 관련 선행연구를 바탕으로 기업의 신정보화 업무환경에서 발생할 수 있는 기술유출의 위협요인을 표1과 같이 사용기기부문, 네트워크환경부문, 어플리케이션 활용부문으로 구분하여 실증분석 하였다.

2.2 관리적 부문의 위협요인

문길주(2006)는 기술정보 보호를 보안기술 측면이외에 보안관리. 출입통제, 교육의 관리적 측면을 분석하였고, 임종인(2011)은 PC나 서버와 스마트폰 사이의 데이터중 민감한 자료가 전송되지 않도록 차단하기 위해 자료의 민감도에 따른 등급 구분을 하여 중요자료는 스마트폰에 저장되지 않도록 하거나 플랫폼에서는 문서가 편집이 불가능한 형태로 변환하는 등의 기업내 보안정책에 신정보화환경을 반영하는 것이 필요함을 관리적 대책으로 제시 했고, 이경복(2011)은 관리적인 측면에서 정보자산의 암호화나 분류의 미흡, 새로운 정보화 환경에서의 보안에 관한 교육 및 훈련의 부재를 지적하였다. 또한 앞으로 부가적으로 제기될 수 있는 보안위협의 요소를 신정보화 도입으로 인한 업무의 협력성 증가의 관점에서도 분석하였다. 특히 클라우드 서비스 환경에서는 개개인의 업무 데이터나 SW가 중앙에 집중되어 언제 어디서나 공유할 수 있게 됨으로써 협업이 용이해 짐으로써 데이터의 훼손이나 중요정보의 노출이 생길 수 있는 가능성이 높아진다는 점을 지적하였다. 본 연구에서는 관리적 측면의 보안실태를 정보화기기의 반출입 통제 여부, 기술정보의 등급관리 여부, 정기적인 보안교육의 실시여부의 항목으로 측정하였다[4],[5],[7].

〈Table 1〉 Related Research about Security Threats

Division	Security Threats	Related Research
User Device	Device Loss/Stolen	H.C. Lee(2011) J.I. Lim(2011) J.H. Ra(2012) E.Y. Jang(2011) K.B. Lee(2011)
	Wiretap /Monitoring	J.H. Ra(2012) E.Y. Jang(2011)
Network	Various Connectable Network	J.I. Lim(2011) K.J. Lee(2013)
	Malicious Code, Hacking	J.H. Ra(2012) J.I. Lim(2011) E.Y. Jang(2011) K.B. Lee(2011)
Application	Easy to connect for Unverified users	K.J. Lee(2013)
	Unverified Application	J.H. Ra(2012)

3. 연구 방법

3.1 조사대상 특성

본 조사의 조사기간은 2013년 1월 14일부터 2013년 2월 22일까지 이며, 최종 유효표본은 1,566개 기업으로 중

1) MDM솔루션은 단말기의 도난 및 분실, 애플리케이션 위변조 체크, 고유 사용자의 단말기 인증, 업무용 앱 사용시 화면 캡쳐 방지, 루팅/탈옥시 서비스차단등의 모바일 보안 기능을 제공함

소기업은 모집단(연구소를 보유한 중소기업)17,392개 중 1,201개 기업을 표집하였고, 비교대조군인 대기업은 65개를 표집하였다.

〈Table 2〉 Sampling Results

Division	Small-medium company	Major company	Total
Poppulation	17,392	-	17,392
Sample Size	1,501	65	1,566

3.2 측정도구

3.2.1 보안인식 측정

신정보화환경에서의 보안인식을 측정하기 위해 사용기기 부문의 보안인식 정도는 사용기기의 도난 및 분실 위협, 도청 및 감청의 위협항목으로 측정하였고, 어플리케이션 활용 부문에서의 보안인식 정도는 모바일 악성코드, 해킹 그리고 미검증 어플 보급에 대해 어느정도 위협을 느끼고 있는지를 5점 척도로 조사하였다.

3.2.2 보안실태 측정

신정보화환경에서의 기술적 보안실태의 측정은 사용기기, 네트워크, 애플리케이션 3개 부문으로 나누어 조사하였다. 사용기기 부문은 스마트폰과 태블릿 PC에 대해 어느정도 보안관리를 하고 있는지를 조사하였고, 네트워크 환경 부문은 무선통신 및 VPN(Virtual Private Network)의 관리 정도를 측정하였고, 애플리케이션 환경 부문은 클라우드를 통한 자료공유에 대한 보안관리와 모바일 오피스 활용에 대한 보안관리 여부를 3점 척도로 조사하였다.

기술적 보안 이외의 관리적 보안실태를 분석하기 위해서 보안정책 및 보안교육에 대한 조사를 실시하였다. 보안정책 부문은 정보화기기의 반출입 통제 여부, 중요자산의 등급별 관리 여부로 조사하였고, 보안 교육 부문은 정기적인 교육이 전직원을 대상으로 실시되고 있는지를 조사하였다.

4. 연구 결과

4.1 신정보화 환경 도입 현황 및 애로사항

신정보화 환경에서의 기술유출 실태 및 보안 대책을 분석하기에 앞서 현재 중소기업에서는 어느 정도 신정보화환경을 업무에 도입하고 있는지 여부와 앞으로의 도입계획 및 도입시 애로사항에 대한 내용을 조사하였다.

신정보화환경을 업무에 활용하고 있는 기업의 비율은 활용중인 기업이 26.9%, 활용 예정 중이거나 고려중인 기업이 39.1%(11.7%+27.4%)인 것으로 나타났다.

〈Table 3〉 Conditions of Using New IT Environment as Company size

Division	Total	Major company	Small-medium company
	1,566	65	1,501
Now Using	421 (26.9%)	26 (40%)	395 (26.3%)
Planned to Use	184 (11.7%)	10 (15.4%)	174 (11.6%)
Considering to Use	429 (27.4%)	14 (21.5%)	415 (27.6%)
No Plan to Use	532 (34%)	15 (23.1%)	517 (34.4%)

기업들이 신정보화 환경을 구축하는데 따른 애로사항으로 응답한 것은 '예산 부족'(60.8%)이 가장 큰 것으로 나타났으며, '전문인력 부재'(41.8%)와 '관련 지식 부족'(36.8%)도 비교적 높게 응답되었다. 그 다음으로 '보안의 위험성'(25.6%), '업무와의 연관성이 떨어져서'(20.4%) 등의 순으로 높게 나타났다.

〈Table 4〉 Difficulties for Implementing New IT Environment

Division	Total	Major company	Small-medium company
	1,566	65	1,501
Lack of Budget	952 (60.8%)	35 (53.8%)	917 (61.1%)
Lack of Specialist	654 (41.8%)	25 (38.5%)	629 (41.9%)
Lack of Knowledge	576 (36.8%)	14 (21.5%)	562 (37.4%)
Security Risk	401 (25.6%)	31 (47.7%)	370 (24.7%)
Lack of Business Relevance	319 (20.4%)	12 (18.5%)	307 (20.5%)
Lack of CEO's Consciousness	156 (10.0%)	10 (15.4%)	146 (9.7%)
No Plan	4 (0.3%)	0 (0.0%)	4 (0.3%)
Etc.	30 (1.9%)	1 (1.5%)	29 (1.9%)

대기업은 신정보화 업무환경 구축에 있어서 '보안의 위험성'(47.7%)을 심각하게 우려하고 있는 것으로 나타났으나, 중소기업은 이러한 위험성(24.7%)보다 '예산 부족'(61.1%), '전문 인력의 부재'(41.9%) 등을 애로사항으로 지적하고 있어 신정보화 환경 구축에 대한 보안 위협에 대한 인식은 대기업에 비해 중소기업은 낮은 것으로 나타났다.

4.2 신정보화환경에서의 보안인식

신정보화환경에서의 보안인식을 측정한 결과는 표5와 같다. 보안인식에 있어서는 대기업과 중소기업의 인식은 크게 차이가 없는 것으로 나타났다.

〈Table 5〉 Cognition of Technology Outflow as Company Size (unit: grade)

Division		Total	Major company	Small -medium company
User Device	Device Loss/Stolen	60.2	56.9	60.3
	Wiretap /Monitoring	60.3	59.2	60.3
Network	Malicious Code	58.7	59.2	58.6
	Hacking	61.0	55.4	61.2
Application	Unverified Application	57.2	56.2	57.3

100점 만점 기준으로 0점에 가까울수록 '심각함', 100점에 가까울수록 '심각하지 않음'을 의미한다. 심각도의 조작적 정의는 표6과 같다.

〈Table 6〉 Operational Definition for Seriousness

	Operational Definition for Seriousness (100 grade scale)				
Seriousness Level	Very Much Serious	Very Serious	Somewhat Serious	Not Very Serious	Not Serious
Grading Scale (Unit: Grade)	0 ~12.5	12.5 ~37.5	37.5 ~62.5	62.5 ~87.5	87.5 ~100.0

부문별 조사결과를 살펴보면, 심각하다는 인식이 가장 큰 측면은 '검증되지 않은 어플리케이션 보급'(57.2점) 측면인 것으로 조사되었고, 다음이 '모바일 악성코드'(58.7점)인 것으로 나타났다.

4.3 신정보화환경에서의 기술적 보안실태

신정보화환경에서의 기술적 보안실태의 측정 결과는 표7과 같다. 가장 관리가 잘 되는 분야는 네트워크 환경인 것으로 조사되었다.

신정보화 환경에 대한 보안 관리 수준은 중소기업보다는 대기업이 높은 것으로 확인되었으며, 특히 대기업의 경우 네트워크 환경에 대한 관리가 매우 잘 되고 있는 것으로 나타났으며(95.4%), 애플리케이션 환경(78.5%)이나 사용기기 부문(72.3%)에 대한 관리도 중소기업 대비 우수하였다. 반면 중소기업의 경우 애플리케이션 환경에 대한 보안 관리(50.6%)가 상대적으로 취약했고, 사용기기에 대한 관리(53.1%)도 낮게 나타났다.

〈Table 7〉 Level of Security Management by Division

Division	Total	Major company	Small -medium company
	1,566	65	1,501
User Device	844 (53.9%)	47 (72.3%)	797 (53.1%)
Network	1099 (70.2%)	62 (95.4%)	1037 (69.1%)
Application	811 (51.8%)	51 (78.5%)	760 (50.6%)

네트워크 환경 부문의 보안 실태를 분석하기 위해서 통신망 분리 운영 여부와 정보시스템의 로그 기록/관리에 관한 질문을 하였다. 외부침입 방지를 위한 통신망 분리 운영 실태에 관한 질문에서 해킹 등 외부침입 방지를 위한 통신망 방어 방안으로 '무선랜 사용시 ID/PW 부여'하는 경우가 43%로 가장 많았고, '내부, 외부 통신망을 분리'하는 경우는 22.8%로 나타났다.

'무선랜 사용에 대한 제한이 없는' 기업도 42.7%로 높은 비중을 차지하였고, 통신망 분리 운영 실태는 대기업과 중소기업간 현격한 차이를 보이는 것으로 나타났다. 중소기업의 경우 '무선랜 사용 시 ID나 PW를 부여'하는 경우는 42.6%이며, 44.1%의 기업은 '무선랜 사용에 아무런 제한이 없는 것'으로 조사되어 외부침입 위험에 많이

노출되어 있는 것으로 나타났다.

〈Table 8〉 Networking Seperation Management

	Total	Major company	Small -medium company
	1,566	65	1,501
In-Out Network Separation	357 (22.8%)	37 (56.9%)	320 (21.3%)
Wireless Usage with ID/PW	674 (43.0%)	35 (53.8%)	639 (42.6%)
No Limitation for Wireless Usage	669 (42.7%)	7 (10.8%)	662 (44.1%)

기술유출 방지를 위해 어떤 솔루션을 이용하고 있는지에 대한 질문에서는 '방화벽'이 48.1%로 가장 많이 활용되는 것으로 나타났으며, 그밖에 'IDS'(7.7%)나 'DLP'(7.3%), 'DRM'(5.6%) 순으로 조사되었으나, 이를 활용하는 기업은 낮은 수준으로 나타났다. 전혀 솔루션을 사용하지 않는다는 기업도 45.8%로 높게 나타났다. 대기업과 중소기업의 솔루션 도입정도를 비교해 보면, 방화벽 활용의 경우 중소기업도 46.8%가 구축을 하고 있는 것으로 나타났으나, IDS, DLP, DRM등의 솔루션 도입률은 대기업에 비해 중소기업은 현저히 떨어지는 것으로 나타났다.

〈Table 9〉 Solution Preparation for Preventing Technology Outflow

	Total	Major company	Small -medium company
	1,566	65	1,501
Firewall	753 (48.1%)	51 (78.5%)	702 (46.8%)
IDS	121 (7.7%)	23 (35.4%)	98 (6.5%)
DLP	114 (7.3%)	21 (32.3%)	93 (6.2%)
DRM	87 (5.6%)	20 (30.8%)	67 (4.5%)
No management	718 (45.8%)	3 (4.6%)	715 (47.6%)

4.4 신정보화환경에서의 관리적 보안실태

신정보화 환경에서 관리적 보안실태에 있어서 정보화 기기 반출입 통제에 관한 운영실태 조사결과, '모든 정보화 기기를 통제'하는 경우는 7.8%로 '일부 기기에 한해 통제'되는 비율은 31.8% 로 나타났다. 기업규모별로 살펴보면, 대기업의 경우 36.9%가 '모든 정보화기기 반출입을 통제'하고, 46.2%가 '일부 기기에 한해 통제'하는 것으로 조사되었지만, 중소기업의 62.3%는 '정보화기기의 반출입 통제를 하지 않는 것'으로 조사되었다.

〈Table 10〉 Entrance Control Condition for User Device

	Total	Major company	Small -medium company
	1,566	65	1,501
Entrance Control for All User Device	122 (7.8%)	24 (36.9%)	98 (6.5%)
Entrance Control for Some User Device	498 (31.8%)	30 (46.2%)	468 (31.2%)
No Entrance Control	946 (60.4%)	11 (16.9%)	935 (62.3%)

보유자산의 등급별 권한관리에 관한 조사에서 응답기업의 28.7%는 '지침에 따라 이행'하고 있었고, 31.9%는 '지침이 수립되어 있지만 이행하고 있지는 않는 것'으로 조사되었다. '관련 지침도 없고, 체계적인 관리조차 없는 기업'은 39.5%를 차지하는 것으로 나타났다

보유자산의 등급별 권한관리는 중소기업과 대기업의 관리정도가 큰 차이를 보이지 않는 것으로 나타나, 중소기업도 대기업대비 비슷한 수준의 관리는 이루어지고 있는 것으로 나타났다.

〈Table 11〉 Management Technology Asset by Grade and Authorization

	Total	Major company	Small -medium company
	1,566	65	1,501
Management with Guideline	449 (28.7%)	45 (69.2%)	404 (26.9%)
No Management despite having Guideline	499 (31.9%)	14 (21.5%)	485 (32.3%)
No Guideline & No Management	618 (39.5%)	6 (9.2%)	612 (40.8%)

직원의 보안교육 실시여부에 대한 조사에서 기업이 직원 보안교육을 실시하는 주기를 살펴보면, '필요할 때

마다 비정기적으로 실시'하는 경우가 79%로 가장 높은 비율을 차지한 반면, '전 직원을 대상으로 한 정기적인 보안교육을 실시'하는 기업은 14.8%로 낮게 나타났다. 기업 규모별로 직원 보안교육 실태를 살펴보면, 대기업은 '전 직원을 대상으로 한 정기적인 보안교육 실시'(44.6%) 비율이 높은 반면, 중소기업은 '필요할 때마다 비정기적으로 보안교육 실시'(80.3%)가 높아 교육형태가 기업규모별로 다르게 나타났다.

〈Table 12〉 Employee Security Training as Company Size

	Total	Major company	Small-medium company
	1,566	65	1,501
Regular Security Training for All Employee	232 (14.8%)	29 (44.6%)	203 (13.5%)
Regular Security Training for Some Employee	85 (5.4%)	4 (6.2%)	81 (5.4%)
Irregular Security Training Sometimes	1,237 (79.0%)	32 (49.2%)	1,205 (80.3%)
No Training	12 (0.8%)	0 (0.0%)	12 (0.8%)

5. 결론

현재 중소기업의 신정보화 환경 구축은 도입기에 있으므로, 구축과 동시에 보안시스템을 함께 갖출 수 있는 지원이 필요하며, 중소기업 자체적 대응이 가능하도록 신정보화 환경에 맞는 보안시스템이 필요하다. 중소기업의 경우 급변하는 정보화환경의 변화에 따른 기술보호 역량을 갖추기에는 한계가 있음으로 정부의 체계적인 보안관리 지원이 요구된다.

5.1 보안관리 측면의 기술유출위협 대응

급격히 증가하고 있는 스마트 단말기는 기술유출의 도구로 활용될 수 있음에도 불구하고 본 조사결과 중소기업은 사용기기의 반출입 통제를 하지 않는 경우가 매우 높게 나타나 신정보화 기기를 통한 기술유출의 가능성이 높아질 것으로 예상됨으로, 모바일 기기에 대한 보안관리 정책적 지원 방안이 요구된다. 특히, 내부직원이 모바일기기를 업무에 사용할 경우 사용자 인증관리 강화 및 사용 기록에 대한 모니터링이 필요하고, 외부방문자의 모바일기기 반출입 통제 규정이 필요한 것으로 나타났다. 기술유출을 막기 위해서는 MDM(Mobile Device Management)솔루션도입과 같은 구체적인 부분의 정부지원이 필요할 것으로 보인다.

고의적, 악의적 기술유출에 대응하기 위해 시스템을 통한 기술정보 생성, 수정, 이동, 삭제에 대한 모니터링 기능을 강화할 필요가 있다.

기본적인 보안관리 솔루션인 방화벽은 중소기업의 경우에도 46.8%가 보유하고 있으나, IDS(침입탐지시스템), DLP(Data Loss Prevent)와 같은 신정보화 환경에서 필요한 보안 시스템 도입률은 중소기업이 대기업 수준에 따라가지 못하고 있는 것으로 나타났다. 또한 문서 단위의 보안을 적용하는 DRM(디지털 저작권 관리 솔루션)은 기술정보유출 방지의 기초적 관리임에도 불구하고 중소기업에서의 도입률은 10%에도 미치지 못하고 있는 것으로 나타났다. 중소기업에서 기술유출 방지와 관련하여 필요로 하는 솔루션 수요조사와 컨설팅을 통해 중소기업 상황에 맞는 정부지원이 필요할 것이다.

5.2 신정보화환경에 대한 보안 인식 제고

정보환경 변화에 따른 기기의 이동성 증가로 인한 기술유출 위협이나, 다양한 어플리케이션보급에 따른 기술유출 위협과 같은 사용자가 인지하지 못한 새로운 위협 요소들에 대한 보안 인식 교육이 필요하다. 새로운 정보환경에 대해 경영자, 현업 종사자, 보안 관리자들은 각각의 위험노출 환경이 다르기 때문에, 교육대상자를 세분화하여 정보환경 변화에 따른 기술유출 위협요인에 대한 보안 인식 교육 및 설명회를 할 필요가 있다. 사용자의 오·남용으로 인한 기술유출 위협에 대응하기 위한 보안교육 및 사용자 인증강화 및 악성코드 대응을 위한 가이드라인 제공이 필요하며, 사용자 접속인증을 강화하기 위한 보안인증서 제도의 도입도 필요할 것이다.

정보화환경의 변화를 반영하여 기존의 기술유출 대응 매뉴얼을 신정보화 환경에 맞추어 재구성할 필요가 있다. 중소기업의 경우 기초적인 보안관리도 실행하지 않는 경우가 30%에 이르고 있으므로, 보안관리의 기본사항을 반영한 가이드라인을 중소기업 규모별(종업원수 기준)로 제공하면서 기업자체의 업무환경에 맞는 보안 관리가 필

요할 것으로 보인다. 또한 정보사용자, 보안관리자 등 각각의 역할에 맞는 매뉴얼을 재구성하여 업무현장에 쉽게 적용할 수 있도록 보급할 필요가 있으며, 기술정보의 등급별 관리를 위한 지침 마련 및 보급이 필요할 것이다.

5.3 시사점 및 한계점

기존의 연구는 신정보화환경에서 유발될 수 있는 정보보안의 위협요인에 관한 탐색적 연구가 주류를 이루고 있으며, 이에 대한 실증분석은 미흡한 실정이었으나, 본 연구는 실증분석을 통해 기업들이 기술유출의 위협요인을 어떻게 인식하고 있으며, 현재 어느정도 관리하고 있는지를 분석하였다. 급격히 변화하는 정보화환경에서 중소기업의 보안관리실태 뿐만 아니라 보안역량 부문의 조사를 위한 체계화된 측정도구 개발이 필요할 것으로 보인다.

REFERENCES

[1] E.Y. Jang, H.J. Kim, C.S. Park, J.Y. Kim & J.I. Lee, The study on a Threat Countermeasure of Mobile Cloud Services, KIISC, Vol 21, No 1, pp.177~186, 2011

[2] H.C. Lee, J.H. Yi, K.W. Sohn, Security Threats and Countermeasures in Smartwork Environment, KIISC REVIEW, Vol.21, No.3, pp.12~21, 2011

[3] J.H. Ra, Y.J. Choi & D. I. Shin, An Exploratory Study on Threats of Smartwork Environment, Journal of Information Technology and Architecture, Vol 9, No. 1, March, pp. 33-42, 2012

[4] J.I. Lim, Security Threats Countermeasures as Changing IT Environment, Journal of Industrial Security, Vol.7, pp.1~73, 2011

[5] K.B. Lee, T.H. Park & J. I. Lim, Security Threats and Countermeasures according to the Environmental changes of Smart Work, The Journal of Digital Policy & Management, Vol. 9, No.4, pp.29~40, 2011.

[6] K.H. Nam, Smart Society IT Trends and Security Threats/Countermeasures, KIISC REVIEW, Vol.22 No.8, 2012

[7] K.J. Lee, Policy Suggestion about Security Threats and Countermeasures in Smart Society, Journal of The Korean Institute of Communication Sciences, Vol.30 No.1, pp.24-32, 2012

[8] K.J. Moon, Security Intension Plan for Research Information -Government Funded Reasearch Center-, KAITS, pp.75-140, 2006

[9] S.K. Rheem, C.K. Lee & J. E. Kim, The Information Security Risks of Smart Age and EU5's Responses, CEM-TP, Vol.7, No.4, pp.135~150, 2011

김 기 호(Kim, Ki Ho)

- 1996년 6월 : 방송통신대학 졸업(경제학)
- 1998년 8월 : 한국외국어대학교 졸업(경영학 석사)
- 2006년 8월 : 한국외국어대학교 졸업(경영학 박사)
- 현재 : 중소기업기술정보진흥원 경영정보화부 부장
- 관심분야 : 정보화, 경영
- E-Mail : kiho@tipa.or.kr

하 규 수(Ha, Kyu Soo)

- 1998년 6월 : 미국 Touro 법과전문대학원 졸업 (J.D.)
- 1999년 6월 : 미국 Georgetown 법과전문대학원 졸업(LL.M.)
- 1998년 8월 : 현재 : 미국 뉴욕주변호사 · 미국 연방변호사
- 2009년 2월 : 한양대학교 경영학과 졸업(경영학박사)
- 2002년 2월 : 현재 호서대학교 벤처전문대학원 교수
- 관심분야 : 법학, 경영
- E-Mail : ksh@hoseo.edu