A Study on Interface Security Enhancement

Joon-Jeong Park†, Sora Kim†, SooHyun Ahn†, Chae-ho Lim‡, Kwangjo Kim§

ABSTRACT

Because the specific security technology alone can not cope with sophisticated attacks, various security management models are applied. But, they do not focus on the vulnerability of the highest part because they offer so many common security management criteria. By analyzing the main information and confidential leakage cases inflicting enormous damage to our society, we found that attackers are using mainly an interface vulnerabilities - the paths that connect the internal and external of the organization, such as e-mail, web server, portable devices, and subcontractor employees. Through this, consider the reality that time and resources to invest in security domain are limited, we point out the interface security vulnerabilities the possibility of attackers to exploit and present a convergence method of security measures. Finally, based of ROI(Return on Investment), we propose the real-time security management system through the intensive and continuous management.

Keywords : Interface security, Real-time security management, Continuous management, ROI(Return on Investment)

조직의 실시간 보안관리 체계 확립을 위한 '인터페이스 보안' 강화에 대한 연구

박준정†, 김소라†, 안수현†, 임채호‡, 김광조§

요 약

특정 보안 기술만으로는 나날이 치밀해지는 공격을 방어할 수 없기 때문에 ISMS(Information Security Management System) 등 다양한 보안관리 모델 등이 적용되고 있지만, 너무 많은 항목에 대한 일반적인 보안관리 방안을 제시하고 있어 취약점이 높은 부분에 집중하지 못하는 단점이 있다. 최근 수년 간 우리사회에 막대한 피해를 입힌 주요 정보 및 기밀 유출 관련 사건을 분석해 본 결과, 공격자는 주로 이메일, 웹 서버, 휴대용 저장매체, 외주업체 직원 등 조직의 내부와 외부를 연결해주는 통로인 '인터페이스(interface)' 취약점을 이용하였음을 발견하였다. 이를 통해 우리는 보안에 투자해야 할 시간과 자원이 제한되는 현실을 고려하여 공격자가 악용할 가능성이 높은 인터페이스에 대한 현재 보안실태를 적시한 후 관리적·기술적·물리적 측면을 융합한 보안대책을 제시하고, 해당 인터페이스에 대한 중점적이고 지속적인 관리(continuous management)를 통해 투자 비용 대비 효과적으로 조직의 실시간 보안관리를 가능하게 하는 체계를 제안하고자 한다.

키워드 : 인터페이스 보안, 실시간 보안관리, 지속적 보안관리, 투자 대비 효과

1. 서 론

IT(Information Technology) 기술이 광범위하게 발달함에 따라 보안 기술도 발전하고 있지만, 특정 보안 기술만으로는 나날이 치밀해지는 공격을 방어하기에 역부족이다. 이에 ISMS(Information Security Management System) 등 다양한 보안관리 모델 등이 적용되고 있지만, 너무 많은 항목에 대한 일반적인 보안관리 방안을 제시하고 있어 취약점이 높은 부분에 집중하지 못하는 단점이 있다. 조직이 원하는 보안수준을 달성하고 기밀자료 유출을 차단하기 위해서는 공격자가 악용할 가능성이 높은 취약점에 대한 집중적인 보안관리가 이루어져야 하는데, 현재 우리나라에서는 그런 시스템을 적용하고 있는 조직을 찾아볼 수 없다.

최근 수년 간 우리사회에 막대한 피해를 입힌 주요 정보 및 기밀 유출 관련 사건을 분석해 본 결과, 공격자는 주로 이메일, 웹 서버, 휴대용 저장매체 등 조직의 내부와 외부를 연결해주는 통로인 '인터페이스(interface)' 취약점을 이용하

※ This work was partly supported by the ICT R&D program of MSIP/IITP, Republic of Korea [1391104001, Research on Communication Technology using Bio-inspired Algorithm] and the KUSTAR-KAIST Institute, KAIST, Korea.
† 준 회 원 : KAIST 정보보호대학원 석사과정
‡ 종신회원 : KAIST 정보보호대학원 초빙교수
§ 비 회 원 : KAIST 전산학부 교수
논문접수 : 2015년 1월 9일
수 정 일 : 1차 2015년 2월 27일
심사완료 : 2012년 2월 28일
* Corresponding Author : Chae-ho Lim(chlim@kaist.ac.kr)

였음을 발견하였다. 이를 통해 우리는 보안에 투자해야 할 시간과 자원이 제한되는 현실을 고려하여 공격자가 악용할 가능성이 높은 인터페이스에 대한 관리적·기술적·물리적 측면을 융합한 보안대책을 제시하고, 해당 인터페이스에 대해 중점적이고 지속적인 관리를 바탕으로 투자 비용 대비 효과적으로 조직의 실시간 보안관리를 가능하게 하는 체계를 제안하고자 하며, 장기적으로는 ISMS 등 다양한 정보보안 관리체계에 인터페이스 보안 강화대책을 적용할 수 있는 방안을 찾고자 한다.

2. 관련 연구 및 동향

2.1 관련 연구

조직의 보안관리를 강화하기 위해 김지숙 등[1]은 민간기업과 공공기관의 정보보호 관리체계 차이에 대해 연구하였으며, 신혜원[2]은 정보유출을 방지하기 위해 내부자 위험도 분석 방법론을 연구하였다. 권오훈 등[3]은 국방망에 대한 효율적인 보안관리 체계에 대해 연구하였고, 김송영 등[4]은 보안사고 모니터링 방법론을 통해 보안정책 변경 근거를 제시하는 연구를 하였다. 그러나 실제 발생한 기밀유출 사례를 통해 공통적으로 취약한 인터페이스를 정의한 후 융합적인 보안대책을 제시하여 지속적이면서도 실시간으로 보안관리를 강화해야 한다는 연구는 진행되지 않았다.

2.2 최근 발생한 주요 기밀 자료 유출 사건

1) 개인정보 유출 등 민간 부문

2011년부터 2014년까지 우리사회에서 이슈가 되었던 대형 개인정보 유출사건 및 사이버 대란 등에 사용된 수단을 분석해 보면 <Table 1>과 같다.

Table 1. The major security incidents

연도	보안사고 발생 업체·기관	수단(대상)
2014	한국수력원자력	USB (외주업체 직원)
2014	판도라TV	웹 서버
2014	카드 3사	USB (외주업체 직원)
2014	농협생명	노트북 (외주업체 직원)
2014	KT	웹 서버
2013	3·20 사이버 테러	웹 서버
2013	6·25 사이버 대란	웹 서버
2012	금융권/방송사 전산망 마비	노트북 (외주업체 직원)
2011	농협 전산망 마비	노트북 (외주업체 직원)
2011	현대캐피탈 정보유출	웹 서버
2011	SK 커뮤니케이션즈 정보유출	웹 서버
2011	△△금융 모의해킹	이메일

2) 산업기밀 관련 부문

2009년부터 2013년까지 적발된 산업기밀 해외 유출 사건은 총 209건이며, 기술유출 주체는 전·현직 직원이 80.4%, 협력업체가 9.6%로 해커의 직접적인 공격이 아니라 조직의 내·외부 연결 통로를 이용할 수 있는 인원이 90%를 차지하였다. 또한 대부분 인터넷 해킹, USB, 스마트폰, 이메일 등의 수단을 활용하여 대규모 정보유출을 시도[5]하고 있다.

산업기밀보호센터에서 공개하고 있는 국내 산업기술 연도별 해외유출 사례를 정리해 보면 <Table 2>와 같다.

Table 2. The major industrial technology leakage incidents

연도	유출된 기술명	수단(대상)
2013	AM-OLED 핵심기술	이메일, USB
2012	세계 최대용량 빌딩용 첨단 에어컨 핵심기술	노트북
2012	태양전지 생산장비 제조 기술	노트북 (협력업체 직원)
2012	차세대 디스플레이 기술	USB (협력업체 직원)
2012	선박 부품 설계 기술	외장 HDD

3) 국방 부문

2013년 방산업체 대상 해킹이 100만 건을 초과[6]하였고 군사기밀 유출이 반복[7]되고 있는 등 우리나라 국방 사이버 위협은 점증하고 있는 상황인데, 공개된 사례를 바탕으로 국방 부문 내·외부 위협에 사용된 수단을 정리해 보면 <Table 3>과 같다.

Table 3. The major security incidents in National Defense

연도	보안사고 내용	수단(대상)
2014	국방부 출입기자 PC 악성코드 감염(3년 간 9회 탐지)[7]	이메일 (출입기자)
2014	안보 관련 기관 주요직위자 PC 악성코드 감염[8]	이메일
2014	방위력개선 관련 기밀 유출[9]	이메일, 메신저
2014	전장망/국방망 바이러스[10]	USB 추정
2013	작전상황도 노출[11]	메신저
2013	군사기밀 탈취[12]	USB (방문객)

3. 인터페이스 보안

3.1 '인터페이스'의 개념 및 중요성

우리는 '인터페이스'를 '조직 내부와 외부를 연결할 수 있는 접합점으로 이메일, 웹 서버, 휴대용 저장매체 및 외주(협력)업체 직원을 포함하는 것'으로 정의한다. 악의적 의도를 가진 비인가자가 이런 인터페이스를 이용하면 (Fig. 1)과 같이 목표 조직의 내부에 손쉽게 침투할 수 있다.

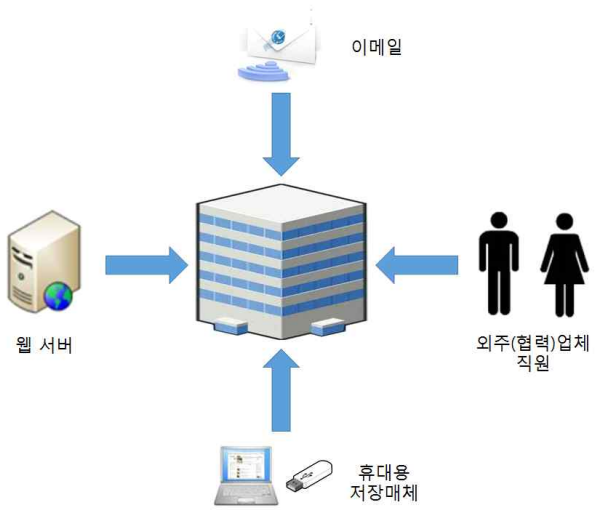


Fig. 1. The paths that can penetrate inside a organization - Interface

보안 영역에서 인터페이스가 중요한 이유는 앞 장에서 살펴본 것과 같이, 공격자는 실제 정보 유출을 시도하기 위해 주로 인터페이스를 활용하고 있는데 대부분 조직에서 인터페이스에 대한 보안관리가 취약해 대형 정보유출 사고 등으로 직결되고 있기 때문이다. 2014년 11월 3일 산업통상자원부에서 발표한 한빛·고리 원자력 발전시설 보안실태 감사결과에 따르면 <Table 4>의 내용처럼 다수의 보안취약점이 식별[14]되었는데, 이 역시 모두 '인터페이스'에 대한 보안관리가 매우 취약하였음을 단적으로 증명해 주고 있다.

Table 4. The security audit result for nuclear power plants

주요 취약점	수단 / 대상
한수원 직원 계정 유출(공유)	협력업체 직원
비인가자 내부시스템 접속	협력업체 직원
비인가자 보안구역 수시 출입	배달업체 직원
미승인 보조기억장치 업무 활용	USB, 협력업체 직원

그런데 주요 정보유출의 창구가 되고 있는 조직의 인터페이스 보안에 대해 우리는 얼마나 관심을 갖고 있는가? 어떤 보안대책을 시행하고 있는가? 중요성을 간과한 채, 단순히 해야 하는 업무라서 관행적으로 이루어지고 있지는 않은가? 인터페이스 보안 실태에 대해 자문해 보고 취약점을 해소하기 위해 어떤 대책을 마련해야 하는지 고민해 보도록 하자.

3.2 인터페이스별 보안취약 실태

1) 이메일

보안에서 핵심이 되면서도 가장 약한 고리는 '최종 사용자[15]'인데 이메일은 피싱과 APT(Advanced Persistent Threat) 등 심리학 및 사회공학적 기법을 활용하여 가장 취약한 고리를 더욱 취약하게 만들 수 있다. 특히, 송·수신에 대한 모니터링 수단 및 통제 정책이 정확히 적용되지 않거나 계정관리에 소홀할 경우 기밀 정보 유출 수단으로 매우 손쉽게 활용될 수 있다.

실제 2012년 '□□□□연구원' 최고위급 임원이 이메일을 이용해 기밀자료를 해외로 유출하다 적발되어 검찰에 구속되고, 2014년 '◇◇◇◇◇◇◇' 퇴직자 이메일 계정을 활용한 해킹 공격으로 인해 전 국민이 불안해하고 국가적인 역량이 불필요하게 낭비된 사례 등에서 알 수 있듯이, 이메일 모니터링 시스템상 작은 허점이 치명적인 보안사고로 직결되고 있는 실정이다.

2) 웹

보안업체의 통계에 따르면, 최근 웹 기반 해킹이 갈수록 증가하여 해킹공격 전체의 47.2%를 차지[16]하는 등 심각한 문제로 대두되고 있다. 또한, 미래창조과학부 점검 결과 포털업체와 웹하드 업체의 홈페이지 역시 보안에 취약[17]한 것으로 확인되었다. 국내 상당수 웹은 설계 단계에서부터 보안을 고려하지 않아 공격자가 악성코드를 간단히 삽입[18]할 수 있는 등 치명적인 취약점을 보유하고 있다.

또한, 사용자가 인식하지 못하는 사이에 워터링 홀(watering hole) 공격 등에 쉽게 노출될 우려가 있고, 본사에 비해 보안수준이 취약한 협력업체 웹 취약점에 침투하여 본사 서버까지 탈취할 가능성이 상존하고 있으나 이에 대한 관심은 높지 않다.

3) USB 등 휴대용 저장매체

USB(Universal Serial Bus) 메모리 스틱, 스마트폰, 노트북 등 휴대용 저장매체는 기밀 유출 의도를 가진 사용자가 타인의 감시에서 벗어나 자료를 절취하는데 활용할 수 있는 수단이며, 반대로 유출 의도가 없는 사용자라도 악성코드 등에 감염된 저장매체를 무분별하게 업무에 활용하면서 본인조차 모르는 사이에 기밀 유출 범죄를 저지를 수 있다.

4) 외주(협력)업체 직원

외주(협력)업체 직원은 해당 조직을 내부자처럼 출입하면서 이메일 / USB 등 다른 인터페이스를 대부분 사용할 수 있어 '인터페이스 중에서도 가장 취약한 인터페이스'이다. 비인가자임에도 핵심 정보시스템에 접속하는 경우도 많고 업무 관련 자료를 개인 휴대용 저장매체에 저장·활용하면서 악성코드 감염으로 인해 기밀자료 유출 및 내부시스템 파괴 등 심각한 피해를 입히는 인터페이스이다.

3.3 인터페이스 보안 강화 방안

인터페이스 보안 취약점에 대해 개별적인 보안기술로 대응하는 것은 대단히 비효율적이다. 모든 구성원들을 대상으로 기술적인 보안대책을 적용함과 동시에 보안교육을 통한 의식 개선, 보안정책 설정, 물리적 차단 등 다양한 수단을 융합한 보안대책을 적용하여 '지속적으로 관리(continuous

monitoring)'하는 것만이 인터페이스 보안을 강화하는 가장 좋은 방법이다.

인터페이스 보안통제 이행 여부를 점검하기 위한 '점검 인터벌(polling time interval)'은 각 조직별로 자산의 중요도와 취약성을 종합적으로 고려하여 결정해야 하며, 인터페이스 보안통제를 적용하기 이전과 이후의 보안수준 변화 과정을 분석해야 한다.

1) 이메일

송신 용량을 제한하여 대량의 정보 유출을 사전 차단하고, 메일 송·수신 상황을 모니터링 할 수 있어야 한다. 또한, 실시간 지속적으로 메일 서버를 검사하여 메일에 첨부된 악성코드 등을 제거하기 위해 노력해야 하며, 퇴직자 등 불필요 인원의 계정은 즉시 삭제하는 등 계정 관리에 만전을 기해야 한다. 이와 더불어, 사적 용무를 위해 메일을 활용하는 빈도를 낮출 수 있도록 사용자들을 교육해야 한다.

특히, 조직의 대표부터 말단 직원에 이르기까지 직위고하와 무관하게 모든 사용자들의 계정을 모니터링 해야 하며, 치명적 기밀유출 사고를 예방하기 위해 단 한 명의 예외조차도 허용해서는 안 된다.

2) 웹

개발 단계에서부터 보안을 고려하여 웹 서버(페이지)를 구성·운영해야 하며, 경량화된 스캔 툴 등을 활용하여 수시로 취약점을 진단하고 발견된 취약점은 즉시 개발자에게 피드백을 주어 오류를 신속히 수정해야 한다. 웹 스캔은 월 1회만 하는 것이 아니라, 매일 1회, 필요시 1일 3회 등 해당 조직의 웹 특성에 맞게 시행해야 한다.

또한, 1개의 백신만을 사용하면서 보안수준을 맹신할 것이 아니라, 기본적으로 국산 백신을 사용하고 외산 백신을 추가 사용하는 등 중복 점검이 가능하도록 시스템을 운영해야 한다. 또한 웹 페이지 접근 권한 설정이 적절한지도 주기적으로 확인·조정해야 한다.

3) USB 등 휴대용 저장매체

보안정책을 설정할 때 업무용 저장매체와 개인용 저장매체를 분명히 구분하여 개인용 저장매체는 업무에 활용하지 못하도록 통제해야 한다. 또한, 업무용 USB는 보안 USB를 사용하여 작업 내역을 지속적으로 감시할 수 있도록 해야 하며, 악성코드 점검 여부 등을 주 1회 이상 수시로 체크해야 한다.

특히 불시 보안점검을 통해 회사자료 유출 여부를 반드시 체크해야 하며, 비인가 저장매체 통제 시스템 적용 여부도 검토할 필요가 있다.

4) 외주(협력)업체 직원

외주업체 직원들에 대해서는 기본적으로 앞에서 살펴본 인터페이스 보안대책을 모두 적용해야 한다. 이에 더하여 보안구역 출입통제를 강화하고 웹 페이지 등에 접근할 수 있는 계정 및 권한을 최소화해야 하며, 각종 보안정책 준수 여부를 주 1회 이상 직·간접적인 수단으로 확인해야 한다. 또한 조직의 보안정책 위반행위가 발견되면 보직조정 등 인사상 불이익과 더불어 외주용역 계약 위반에 대한 민·형사상 책임을 부과할 것임을 수시로 주지시켜야 한다.

4. 인터페이스 보안을 강화한 실시간 보안관리

4.1 인터페이스 보안 Simulation 결과

2010년 9월 ~ 12월 간 '한국원자력연구원'은 보안통제 구현과 관리 상황을 분석한 바 있다. 이를 대상으로 해당 조직 특성에 부합하도록 보안통제 항목 및 지표를 구성하여 수준을 측정해 본 결과, (Fig. 2)와 같이 인터페이스 보안에 해당하는 '접근제어' 항목의 수준이 가장 낮았다. 이에, '접근제어' 분야를 집중적으로 보완한 결과 매월 해당 분야 수준이 향상되고, 그에 따라 '한국원자력연구원'의 전반적인 보안수준이 향상됨을 확인할 수 있었다.

11월의 경우, 원인을 파악하지 못한 침해사고가 발생하여 평균값이 다소 하락하였으나, 보안수준이 향상되는 전반적인 추세는 확인할 수 있었다.

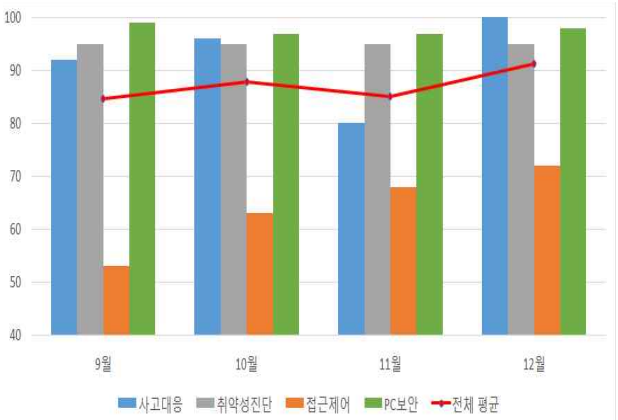


Fig. 2. Simulation results for Korea Atomic Energy Research Institute

4.2 기존 정보보안 관련 분야 관리모델의 한계

국가사이버안전센터는 국가 기관을 대상으로 정보보안 관리실태 평가를 시행하고 있는데 총 6개 분야 29개 지표 129개 항목을 평가하고 있다[19]. 한국인터넷진흥원은 정보보호 관리체계 인증을 통해 18개 통제 분야 104개 통제 항목[20], 254개 세부 점검 항목[21]에 대해 심사한다.

정보보안의 제반 영역에 대해 과도하게 많은 지표를 동일한 주기로 평가하고, 대상 기관은 해당 주기에 맞게만 보안업무를 수행하면 보안수준이 높은 것으로 평가된다. 하지만 이 경우 공격자의 공격 가능성에 대비한 해당 기관의 실제적 보안수준이 높다고 볼 수 없는 한계가 있으며, 모든 보안통제 항목에 대한 통제를 강화하는 것 역시 소요되는 노력과 비용 측면에서 비효율적이라 할 수 있다.

4.3 인터페이스 보안 강화 방안 적용 제안

평소 기관(업체)별로 해당되는 정보보안 관리모델을 바탕으로 보안업무를 수행하면서, 조직의 특성에 따라 취약점이 더 높을 것으로 우려되는 인터페이스를 식별한 후 해당 인터페이스에 대해 융합적인 보안대책을 적용하고 보안관리 주기를 조정(예 : 월 1회 → 주 1회 / 실시간)하여 지속적으로 관리해야 한다.

'보안 격차'는 '보안 위협'과 '현재 보안 수준'의 차이로 정의할 수 있고, 이 보안 격차에 의해 조직의 보안 수준을 판단할 수 있다. 적절한 보안관리를 실시하지 않을 경우 시간이 경과함에 따라 보안 격차가 커지는데 반해, 지속적인 보안관리를 시행할 경우 보안 격차를 최소화하면서 조직의 보안 수준도 향상시킬 수 있다.

한편, 정보보안 수준 측정 시스템을 발전시키기 위해서는 필요한 데이터를 쉽게 얻을 수 있어야 하는데[22], 보안 수준에 결정적 영향을 미치는 인터페이스에 대한 지속적인 모니터링을 통해 원시 데이터(raw data)를 수시로 수집하면 실시간 보안관리를 구현하고 보안수준 평가 체계를 손쉽게 구축・이행할 수 있다.

본 고에서는 현재 우리나라에서 정보보호 관리체계 인증 관련 분야에서 가장 보편적으로 활용되고 있는 'ISMS 인증 심사 기준[21]'을 예로 들어 발전방안을 제안한다. <Table 5>는 상기 기준에 명시된 ISMS 18개 통제 분야 중 「10. 접근통제」 분야에 해당하는 주요 점검 항목을 나타내고 있다.

Table 5. The main inspection items of the 'Access Control' field in the ISMS

통제 분야 (통제 분야 번호)	주요 점검 항목
접근통제 정책 (10.1)	접근통제 영역을 정의하고 접근통제 영역별로 접근통제 정책을 수립하고 있는가?
접근권한 관리 (10.2)	외부자에게 부여하는 계정은 한시적으로 부여하고 사용이 끝난 후에는 삭제 또는 정지하고 있는가?
사용자 인증 및 식별(10.3)	정보시스템 및 정보보호시스템에 대한 안전한 사용자 패스워드 관리절차를 수립・이행하고 있는가?
접근통제 영역 (10.4)	**접근통제 정책에 따라 분리된 네트워크 영역 간에 접근통제를 하고 있는가?**
	서버의 사용목적과 관계없는 서비스를 제거하고 있는가?

현행 ISMS 점검 항목의 상당수는 명시된 보안통제에 대해 1회성으로 이행 여부만을 점검할 뿐, 보안수준 향상을 위해 지속적・정기적으로 보안활동을 수행하는 것에 주안점을 두고 있지 않다. 또한, 계량화된 데이터를 확보할 수 있는 분야가 상당함에도 불구하고 보안 관련 원시 데이터를 확보하여 조직의 보안수준을 객관적으로 평가・관리하는 개념을 적용하지 않고 있는 한계점을 보완해야 한다.

예를 들어 '네트워크 트래픽 감시를 위한 침입탐지시스템 유지・관리 여부' 등과 같이 정성적으로 평가해야 하는 부분도 있지만, 정량적으로 평가할 수 있는 항목은 최대한 원시 데이터를 많이 확보한다면 해당 조직의 보안수준을 객관적 지표를 통해 실시간으로 판단할 수 있다.

또한, 이전 평가 실적과 비교・분석할 수 있기 때문에 ISMS 인증 후에도 해당 조직 자체 역량으로 지속적으로 관리할 수 있는 우수한 정보보안 관리시스템이 될 것이다. 한편, 보안부서 최고 책임자는 이를 보고받아 분석하여 조직의 보안 위협과 취약점을 진단하고 장기적인 발전방안을 마련하는데 활용할 수 있다. 또한, 침해사고 등 긴급상황 발생 시 대응 시간 역시 줄일 수 있는 효과가 있을 것으로 사료된다.

<Table 6>은 상기 ISMS 「10. 접근통제」 분야 중 '10.4 접근통제 영역' 주요 점검 항목을 재구성한 것이다. 각 통제 항목별로 점검해야하는 내용과 이에 대한 측정 공식, 측정 주기 및 보고 주기를 포함하고 있다.

Table 6. Advanced inspection standards(example)

구 분		세부 내용
통제 항목	1	네트워크 접근 통제
	2	서버 접근 통제
점검 내용	1	접근통제 정책 준수율(%)
	2	불필요 서비스 제거율(%)
측정 공식	1	(1 - 비인가 접근 수 / 전체 접근 수) × 100
	2	(서비스 제거 수 / 전체 서비스 수) × 100
측정 주기	1	주 1회 이상
	2	월 1회 이상
보고 주기	1	월 1회
	2	분기 1회

위와 같이 조직의 보안 취약 요인에 대한 지속적인 보안관리를 통해 조직 전체의 보안업무가 튼튼한 기초 위에서 유기적으로 수행되는 가운데 반드시 집중해야 하는 취약점, 기밀 유출 우려가 높은 인터페이스에 맞춤형으로 대응하는 시스템을 구축할 수 있어 투자 비용 대비 효과적인 보안업무 수행[23]이 가능하다.

5. 결론 및 향후 연구

우리는 최근 이슈가 된 정보 및 기밀 유출 사례를 분석하여 공격의 주요 통로가 된 '인터페이스'를 식별한 후 보안 취약점과 대응방안에 대해 연구하였다.

조직의 기밀 정보 유출을 차단하기 위해 취약한 인터페이스별 보안대책을 제시하였으며, '방어자가 모든 공격을 방어해야 한다는 것은 가능하지도 않고 필요하지도 않다[24]'는 최근 추세에 부합하게, 투자 비용 대비 효과적인 보안업무를 수행할 수 있도록 ISMS에 인터페이스 보안 취약점을 지속적으로 관리할 수 있는 방안을 제안하였다.

앞으로는 향후 공격자가 악용할 가능성이 높은 인터페이스에 대해 추가적으로 연구하고, 조직의 다양한 보안 분야 전체 위험도 중에서 인터페이스 보안이 차지하는 비율도 분석할 예정이다.

또한, 실제 ISMS 등 다양한 정보보안 관리모델에 인터페이스 보안 강화 방안을 적용한 체계를 구현하기 위해 구체적인 항목 및 지표를 재구성할 것이다. 수집된 인터페이스 보안 준수 데이터의 적절성(Effectiveness, Efficiency, Compliance) 확인 및 갱신 프로세스를 추가할 것이며, 데이터의 무결성과 변조 유무, 거짓 보고 등을 감사(audit)하는 프로세스를 추가한 후 실제 조직에 적용하여 효과성을 파악하는 등 실시간 보안관리가 가능토록 개선할 것이다.

References

[1] Ji-sook Kim *et al.*, "Comparison of The ISMS Difference for Private and Public Sector," *Journal of Korea Institute of Information Security and Cryptology*, vol. 20, no. 2, pp. 117-129, April 2010.

[2] Hyewon Shin, "Methodology to Analyze Insider Risk for the Prevention of Corporate Data Leakage," *Korea Computer Congress 2012*, vol. 39, no. 1, pp. 295-297, June 2012.

[3] Oh-Hun Kwon *et al.*, "A Persistent and Real Time Security Management System for Korea Military Network," *Journal of Korea Institute of Information Security and Cryptology*, vol. 23, no. 6, pp. 54-66, Dec. 2013.

[4] Song-young Kim *et al.*, "A study on the security policy improvement using the big data," *Journal of Korea Institute of Information Security and Cryptology*, vol. 23, no. 5, pp. 969-976, Oct. 2013.

[5] National Industrial Security Center[Internet], http://service12.nis.go.kr/servlet/page?cmd=preservation&cd_code=outflow_1&menu=AAA00#.VD47J01xlZQ, 2014.

[6] Munhwailbo[Internet], http://www.munhwa.com/news/view.html?no=2014100801071023173002O, 2014.

[7] Joon-Jeong Park and Kwangjo Kim, "A Compensation Method to the Deliberate Military Secret Leakers," *Conference on Information Security and Cryptology-Winter 2014*, Dec. 2014.

[8] YounhapnewsTV[Internet], http://www.news-y.co.kr/MYH20140822016200038, 2014.

[9] Ministry of Science, ICT and Future Planning[Internet], http://www.msip.go.kr/www/brd/m_211/view.do?seq=1251, 2014.

[10] Prosecution Service[Internet], http://www.spo.go.kr/seoul/notice/notice/notice01.jsp?mode=view&board_no=116&article_no=579011, 2014.

[11] SBS[Internet], http://news.sbs.co.kr/news/endPage.do?news_id=N1002623091&plink=ORI, 2014.

[12] YTN[Internet], http://www.ytn.co.kr/_ln/0103201310141055339751, 2014.

[13] AJU Business Daily[Internet], http://www.ajunews.com/common/redirect.jsp?newsId=20121023000324, 2012.

[14] Ministry of Trade, Industry & Energy[Internet], http://www.motie.go.kr/motie/ne/presse/press2/bbs/bbsView.do?bbs_cd_n=81&bbs_seq_n=156671, 2014.

[15] R. West, "The Psychology of Security : why do good users make bad decisions?," *Communications of the ACM*, 51(4), pp. 34-40, April 2008.

[16] Boannews[Internet], http://www.boannews.com/media/view.asp?idx=40482&kind=1, 2014.

[17] Ministry of Science, ICT and Future Planning[Internet], http://www.msip.go.kr/www/brd/m_211/view.do?seq=1228, 2014.

[18] AJUnews[Internet], http://www.ajunews.com/view/20141016093217871, 2014.

[19] National Cyber Security Center, "Introduction to G-ISMS," *Journal of Korea Institute of Information Security and Cryptology*, vol. 23, no. 5, pp. 9-11. Oct. 2013.

[20] Korea Internet and Security Agency[Internet], http://isms.kisa.or.kr/kor/intro/intro02.jsp, 2014.

[21] Korea Internet and Security Agency[Internet], http://isms.kisa.or.kr/kor/notice/dataView.jsp?p_No=48&b_No=48&d_No=114&cgubun=&cPage=1&searchType=ALL&searchKeyword=, 2013.

[22] NIST, *Special Publication 800-55 Revision1: Performance Measurement Guide for Information Security*, "http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf"

[23] Chae-ho Lim, "Cyber attack strategy(NaverCast) [Internet]," http://navercast.naver.com/author_contents_list.nhn?acknowledgeType=author&acknowledgeId=au1337, 2014.

[24] C. Herley, "Security, Cybercrime, and Scale," *Communications of the ACM*, 57(9), pp. 64-71, Sep. 2014.

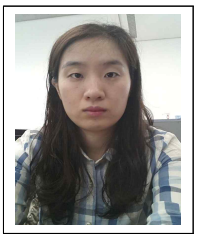
박 준 정

e-mail : sunsun64@kaist.ac.kr

2004년 육군사관학교 지휘행동학과(학사)

2014년~현 재 KAIST 정보보호대학원 (석사과정)

관심분야 : 정보보호 정책 및 법률



김 소 라

e-mail : c15460@kaist.ac.kr
2008년 육군사관학교 운영분석학과(학사)
2013년~현 재 KAIST 정보보호대학원 (석사과정)
관심분야 : 악성 도메인 탐지

안 수 현

e-mail : ahn1015@kaist.ac.kr
2014년 숭실대학교 정보통신전자공학부(학사)
2014년~현 재 KAIST 정보보호대학원 (석사과정)
관심분야 : 네트워크 보안, 자동차 보안

임 채 호

e-mail : chlim@kaist.ac.kr
1986년 홍익대학교 전산학과(학사)
2001년 홍익대학교 전자계산학과(박사)
2006년~2009년 (주)NHN 보안실장, 연구센터 수석
2009년 한국정보보호학회 부회장
2010년~현 재 KAIST 사이버보안연구센터 연구부소장
2010년~현 재 KAIST 정보보호대학원 초빙교수
관심분야 : 인터넷 보안, 정보보호 위험 관리, 정보보호 관리 및 정책

김 광 조

e-mail : kkj@kaist.ac.kr
1980년 연세대학교 전자공학과(학사)
1983년 연세대학교 전자공학과(석사)
1991년 일본 요코하마 국립대학교 전자정보공학(박사)
1999년~2004년 세계암호학회(IACR) 이사
2005년~2008년 ASIACRYPT 조정위원회 의장
2006년~2009년 한국정보통신대학교(ICU) 공학부장
2009년 한국정보보호학회(KIISC) 학회장
2009년~현 재 KAIST 전산학부 교수
2010년~현 재 한국정보보호학회(KIISC) 명예회장
2014년~현 재 국제정보처리연합 정보보호위원회(IFIP TC-11) 한국대표
관심분야 : 암호와 정보보호 이론 및 응용