국가안보를 위한 공공기관의 내부자 정보 유출 예방대책: 사이버 안보·형사정책 관점

최관* · 김민지**

요 약

이 연구는 사이버 안보 및 형사정책 관점에서 공공기관의 내부자 정보유출에 대한 예방대책을 제시하는 것이 목적이다. 이를 위해 2장에서는 공공기관 정보보안시스템의 정의 및 이용현황에 대해서 살펴보았고, 3장에서는 웹서비스 기반 정보유출과 악성코드 기반 정보유출에 대해서 살펴보고, 국가안보적 측면에서 2014년에 발생했던 3대 카드사 개인정보유출사건에 대한 사례분석을 정보유출과 내부자의 연관성 측면에서 분석하였다. 4장에서는 본 연구의 대책으로서 크게 4가지를 제시하였는데 첫째, 사용자 기반 웹 필터링 솔루션을 통한 정보유출 차단으로서 악성코드에 대한 노출빈도를 제한하며, 개인정보가 포함된 경우 역시 차단하는 기능을 가지고 있다. 둘째, 악성코드에 의한 정보유출을 예방하기 위해 백신 및 백신관리시스템을 도입하여야 한다. 셋째, 전용 악성코드에 의한 정보유출을 차단하기 위해 내부망에서의 이동식 매체 사용을 자제하고, 해당 악성코드에 맞는 전용백신을 주기적으로 활용하여야 한다. 넷째, 스마트폰용 악성코드로부터 정보유출을 예방하기 위해 암호화 어플리케이션을 활용하여 중요 정보에 대한 암호화 저장이 이루어져야 한다.

Issues and Preventions of Insider Information Leakages in Public Agencies for National Security: Cyber Security and Criminal Justice Perspectives

Choi Kwan* · Kim Minchi**

ABSTRACT

The purpose of this study is to provide implications for preventing insider information leakages in public agencies for national security. First, the study examined the definitions and current usage of information security systems of public agencies were examined. Second, web-service base information leaks and malware-base information leaks were discussed and three major credit card companies' personal information leakage cases were analyzed. Based on the analysis, four solutions were provided. First, information leakages can be protected by using web filtering solutions based on the user, which make possible to limit frequencies of malware exposures. Second, vaccine programs and vaccine management system should be implemented to prevent information leakages by malware. Third, limit the use of portable devices within local networks to prevent information leakages and vaccines programs for malware should be regularly used. Forth, to prevent information leakages by smartphone malwares, data encryption application should be used to encrypt important information.

Key words : Insider Information Leakage, Information Security System, Prevention, National Security, Criminal Justice

접수일(2016년 12월 1일), 게재확정일(2016년 12월 30일)

* 삼성교통안전연구소 책임연구위원, (주저자)

** 숙명여자대학교 사회심리학과 교수 (교신저자)

1. 서 론

한국은 정보통신기술 발달과 함께 공공기관 및 기업의 업무환경이 IT를 기반으로 한 구조로 변화하여 많은 정보들이 디지털화 되었다. 한국은 2014년 유엔 전자정부평가(UN E-Government Survey 2014)에서 3회 연속(2010, 2012, 2014 등) 세계 1위라는 영애를 수상하였다[2]. 이는 공공정보의 개방 및 공유로 인한 투명성 제고, “민원24”와 “홈택스”와 같은 시스템의 연계 및 통합을 기반으로 한 서비스전자정부로 인해 업무환경이 IT를 기반으로 변화하면서 자연스럽게 내부자에 의한 개인정보 그리고 주요산업기술의 탈취 그리고 위·변조 또는 유출 등의 위험증가와 함께 정보보안(Information Security)에 대한 중요성 역시 강조되고 있다. 이 연구의 목적은 국가안보 측면에서 공공기관에서 보안 관리와 관련하여 내부자에 의한 주요기술유출문제에 대해 분석하고 이에 대한 예방대책에 대해 살펴보는 것이다.

2. 공공기관 정보보안시스템의 정의 및 이용현황

정보보호시스템(Information Security System)의 의미는 있는 정보, 시스템, 그리고 이를 포괄하는 네트워크를 외부침입 및 감염으로부터 보호하는 것이 목적인 보안시스템이다[6][22]. 예를 들어, 국민안전처는 정보시스템이 보유중인 정보유출, 위조·변조, 훼손 등 정상적인 서비스방해목적으로부터 해당 정보를 보존하기 위한 장치 및 프로그램으로 규정한다[15].

법무부의 경우, IT기술을 형사사법시스템에 도입하여, 수사・기소・재판・형집행 등 형사사법 전 과정을 전자적 방법에 근거하여 처리함으로써 투명하고 정확한 형사사법절차 구현을 위해 만들어진 형사사법정보시스템(KICS : Korea Information System of Criminal Justice Services)등이 있다[14].

2013년부터 정부기관들이 다양한 형태의 정보보호 위협요인으로부터 내부정보보호를 위해 서비스를 활용하고 있는데, 조사 대상기관의 90% 이상이 정보보안을 목적으로 활용하는 서비스는 “안티바이러스”와 “침입차단시스템”, “보안USB도구” 등 기타서비스 등으로 나타났고, 80% 이상이 보안관리시스템, 침입방지시스템, DDoS 대응장비를 운영하고 있었다[11].

3. 내부자에 의한 정보유출 분석

3.1 웹서비스 기반 정보 유출

웹서비스 기반 정보유출에서 검색엔진의 경우 시민들이 알고자 하는 정보를 손쉽고 신속하게 수집할 수 있다는 긍정적인 측면이 있지만, 반면에 이를 악용하여 개개인들의 개인정보를 불법적으로 습득하는데 활용될 수 있다[11]. 검색엔진을 기반으로 특정한 인터넷 사이트를 중심으로 하는 옵션에서 시작하여 특정 문자열과 함께하는 페이지까지 다양한 검색이 가능하고, 또한 해당 검색엔진성능의 고도화로 인해 해당 시스템의 주요 정보 그리고 추가적인 민간정보에 대한 접근 경로까지 확인가능하게 되었다[20].

결론적으로, 상기의 Data만 가지고도 특정한 사이트의 취약점을 선제적으로 찾아내고 이어, 개인정보(성명, 나이, 주민등록번호 등) 및 기업정보들(내부 회계자료, 내부 직원정보 등) 역시 검색이 가능하다[15].

예를 들어, 2016년 현재 대부분의 중국 웹사이트들에서 한국 온라인 게임계정을 쉽게 생성하는 방법에 대해서 검색 및 생성방법을 문의하는 글이 많이 올라오는 사이트가 있는데, 한국은 대부분의 인터넷사이트들이 주민등록번호 없이 회원가입이 불가능하기 때문에 해당 사이트가입을 목적으로 한국인들에게만 존재하는 주민등록번호를 인터넷상에서 서로 공유할 뿐만 아니라, 민간기업의 게시판이나 학회 홈페이지의 게시판을 통해 첨부된 개인정보들이 사이트를 통한 검색이 가능하기 때문에 이에 대한 주의가 요구된다.

3.2 악성코드 기반 정보 유출

정보유출문제들 중에서 악성코드에 기반을 둔 해킹범죄 역시 많이 발생한다. 악성코드 기반 정보유출범죄는 보통 정보사용자들의 개인정보, 금융정보 같은 중요 정보수집을 목적으로 대부분 발생한다[8]. 악성코드는 2016년 현재 발전을 거듭하여 초창기 수동적

으로 전파되던 바이러스와 다르게 메신저 그리고 USB 및 전자 우편 또는 문자메시지 등 다양한 방법들로 펴져나가고 있다. 최근 악성코드 기반 정보유출의 문제점은 과거에 자신의 실력을 증명하기 위한 성향에서 금전적 이익을 주된 목적으로 발생하고 있다[7].

악성코드전염을 목적으로 퍼지는 방법의 경우, 주로 해킹된 웹 페이지나 개인 전자 우편, 문자메시지에 의해 감염이 발생한다. 전자 우편은 주로 세월호사건과 같은 시대적으로 사회적 충격을 가지거나 가졌던 내용들을 수단으로 하여 해당 내용을 첨부한 메일을 사용자가 확인을 위해 열게 되면, 그 즉시 악성코드에 감염되는 형태이다. 또한 웹 페이지에 의한 악성코드 전파는 해킹을 시도하는 범죄자가 해당 웹사이트를 해킹하고 방문자들을 대상으로 자동으로 악성코드가 다운로드 되도록 하여 감염되게 하는 것이다[14].

2010년부터 급증하는 스마트폰 상용화로 스마트폰을 위한 악성코드 역시 증가하고 있다[8]. 스마트폰 기술발전 이전에는 컴퓨터와 스마트폰의 영역이 별개로 인식되었지만, 스마트폰이 점점 여러 기능을 포괄하는 개념으로 변하면서 특성인 통화내역, 전화번호, 문자메시지 등과 같은 개인정보들을 노린 악성코드에 감염될 위험이 증가하고 있다.

3.3 사례분석: 3대 카드사 개인정보 유출사건

3.3.1 피해사례

2014년 1월, 발생한 내부정보 유출사고는 3대 카드사(KB국민카드, 롯데카드, NH농협카드)가 보유 중인 1억400만 건 이상의 고객정보가 외부용역직원에 의해 유출되었다. 유출된 정보는 단순개인정보(성명, 휴대전화번호, 자택 주소 등)와 심각한 금융정보(카드번호, 결제계좌정보 등)까지 포함되었다. 피해를 입은 고객들은 카드 해지 및 재발급을 요청하였고, 관련된 임직원들은 중징계를 받았다. 이를 계기로 하여 정보보안의 중요성에 따라 다양한 정책들이 도입되었다.

한국정부는 2014년 3월 발표한 '금융분야 개인정보 유출 재발방지 종합대책' 등에 근거하여 단계적으로 개인정보보안이 강화되면서 금융회사를 포함한 많은 민간회사들이 업무 관련하여 최소한의 개인정보만을 필수 항목으로 수집하게 되었다.

결론적으로, 내부자(전·현직 및 협력업체 직원)에 의한 위협은 네트워크뿐만 아니라 기반 시설과 관련된 보안에서 무엇보다도 심각한 위협으로 간주되고 있으며, 해당 조직이 보유한 정보 및 데이터 유출은 외부자에 의해 발생하는 것보다 내부자에 의해서 많이 발생하는 것으로 나타났다.

3.3.2 정보유출과 내부자의 연관성

공공 및 민간기업에서 만들어지는 대부분의 전자문서들은 해당 기관의 중요자산으로 규정된 절차가 없이는 외부 유출을 엄격히 제한하여야 한다. 기관 및 기업의 주요사업에 대한 계획서 혹은 기밀문서 또는 개인정보나 기술력이 포함된 설계도면 등은 적법한 절차 없이 외부로 유출이 발생할 경우 심각한 경제적 피해뿐만 아니라 해당 조직의 존립과도 직결될 수 있을 정도로 엄청난 파급효과를 지니고 있다. 또한, 현대사회에는 내부자에 의해 발생하는 정보유출문제를 얼마나 효과적으로 억제하고 예방하는가 하는 문제가 해당조직의 평가와 성장에 중요한 영향을 미친다.

내부정보유출과 관련해 최근의 동향은 유출경로의 변화이다. 과거에는 해커에 의한 외부침입사례가 대부분이었다면, 최근에는 내부자에 의한 정보유출이 심각하다[16]. 개인들이 소지한 모바일 단말기를 회사업무에 활용하는 BYOD(Bring Your Own Device) 문화가 정착 및 확산됨에 따라 주요내부정보가 유출될 기회가 증가하였으며, 기술발달에 근거한 전산기기의 소형화로 인해 보안사고의 가능성 역시 증가하였다.

결론적으로 내부자에 의한 정보유출은 산업스파이 활동과 직접적인 관련이 있는데 주요 기술 및 회사정보가 경쟁업체에 불법적으로 습득되면서 여러 가지 피해가 발생하게 되며, 나아가 금융, 의료, 통신 등 고객 개인정보를 대량으로 취급하는 업종의 경우, 해당 조직뿐만 아니라 많은 수의 피해자가 추가로 발생하게 된다. 이와 같이 내부정보 유출문제는 해당 피해가 해킹 등 외부공격에 버금가기 때문에 사전예방이 중요하게 된다. 내부자에 의한 정보유출은 일반적으로 ①의도성 유출과 ②비의도성 유출로 구분할 수 있다. 먼저, 의도성 유출은 의식적·불법적 목적을 위해 정보를 무단 취급하는 것이며, 비의도성 유출은 의도치 않게 정보누출이 이루어지는 것이다[16].

결국, 의도성의 유무를 떠나 기업에는 큰 피해를 끼치게 되므로 기업 보안담당자는 모든 상황을 고려한 보안 관리계획을 만들어야 한다. 무차별적인 개인정보 수집보다 DB보안 프로그램, 암호화 소프트웨어를 통한 보안조치를 우선 고려할 필요가 있다.

4. 예방대책

4.1 사용자 기반 웹 필터링 솔루션을 통한 정보유출 예방

2016년 한국인터넷진흥원(KISA)에 의하면, 2015년 대비 '커뮤니티 웹사이트'를 통한 악성코드 유포(11%→26%)가 심각한 것으로 조사되었다[26]. 그러므로 웹 필터링을 통해 정보유출을 예방할 필요가 있다. 일반적인, 웹 필터링(Web Filtering)은 위험으로 인식된 웹 사이트에 대한 접근차단을 위한 기술로서, 네트워크 대역폭 확보와 함께 악성 코드에 대한 노출빈도 역시 제한한다. 그리고 웹 페이지로 작성되는 내용과 관련해 개인정보가 포함되어 있는 경우와 불건전한 음란물 및 광고 역시함께 차단하는 기능을 가지고 있다. 그러나 기존의 웹 필터링 기술은 단순히, URL에 사용자 IP요청을 제한, 응용프로그램에서 제한 등의 제공하였지만[17], 사용자 기반 웹 필터링은 사용자별 요청 제한, 글 읽기·쓰기에 대한 제한, 이미지에 대한 제한, 전자 우편 및 사용자 정보에 대한 설정, 요청 횟수 제한 등 사용자별 요청 정도를 구분가능하며 공격자와 사용자에 대한 구분이 능하여 웹 서비스 방어에 효과적으로 대응할 수 있다. 실증 연구 결과, 게시판·블로그·로그인·회원가입 등에 적용한 결과 공격요청에 대한 "사전차단", "특정정보의 제사용 방지", "공격요청 사전 차단", "스팸 도배 방지" 등의 효과가 있는 것으로 나타났으므로[3], 공공기관에서는 사용자 기반의 보안점검 및 웹 필터링을 통하여 정보유출에 효과적으로 대응하여야 한다.

4.2 악성코드를 이용한 정보유출 차단

악성코드에 의한 정보유출 차단을 위해 실시간 감시 및 탐지가 가능한 백신 및 백신관리 시스템을 활용하여야 한다[12]. 현재 악성코드 탐지 법으로는 해시 값, 문자열 검사, 제네릭 기법, 행위탐지 기법 등이 있지만, 악성코드가 발생되어도 개발자와 유포자는 같은 악성코드를 그대로 사용하지 않고 일부 쓰레기 코드를 추가하거나 패킹을 하여 악성코드가 탐지되지 않도록 한다. 그리고 시그니처가 증가할수록 시스템 리소스메모리 차지도 증가하여 탐지속도가 느려지는 문제점 역시 존재한다. 2016년 7월 인터넷진흥원은 악성코드에 취약한 소프트웨어 순서로서 Adobe Flash Player, Java Applet, MS OLE, MS Internet Explorer 순으로 대부분 MS 윈도우에 초점이 맞추어져 있었다. 그 결과, 대부분의 악성코드 들은 윈도우 파일 형태인 PE 구조로 이루어져 있다[17]. 그러므로 파일구조(Dos Stub, Section Size, Compile Time, Section Naming, Entry Point, Section Permission, Overlay, IAT Patch, Forwarding EAT, Section Entropy)에 기반을 둔 악성코드 탐지방법을 활용할 필요가 있으며 실제로 적용결과 86.7%의 높은 탐지율을 보인 것으로 나타났으므로 파일구조에 기반을 둔 악성코드탐지기법을 통해 정보유출의 효율성을 증대시킬 필요가 있다[11].

4.3 이동식 매체 통한 악성코드 전파 및 정보유출 예방

일반적으로 폐쇄망을 사용하는 조직에서는 외부에서 악성코드가 유입될 가능성이 없다고 판단할 수 있다. 하지만 망 분리로 인한 이동식매체 사용증가로 각종 데이터 및 정보들이 유통 가능하므로 주의해야 한다[9]. 이동식 매체가 가지는 특성상 한 컴퓨터에서만 사용이 이루어지는 것이 아니고 여러 컴퓨터를 돌아가며 사용할 수 있으므로 악성코드에 손쉽게 노출될 수 있으며, 네트워크로 연결될 시, 사내 메신저 혹은 네트워크를 기반으로 빠르게 전파될 수 있다.

오토런(Autorun) 악성코드가 대표적인 예로, 이 악성코드에 감염되면 Windows Explorer에서 오른쪽 버튼을 눌렀을 때 메뉴에서 글씨가 깨져 나오며, 숨김 파일 및 폴더 표시, 보호된 운용체계(OS) 파일 숨기기 설정 변경이 불가능하다. 그리고 내 컴퓨터에서 저장장치를 누르면 새 창에서 열리고 USB, 외장하드, 휴대폰, 메모리카드 등이 감염되면 'autorun.inf' 파일과 정체를 알 수 없는 실행 파일이 생성된다[26]. 201

6년 최근의 오토런 악성코드는 자바스크립트나 윈도 스크립트로 작성됐으며, 분석을 어렵게 하도록 난독화 했다[25]. 예를 들어, 악성코드 탐지방해를 위해 분석 도구, 레지스트리 편집기, 시스템 구성 프로그램 등의 보안활동이 실행되면 즉시 종료시킨다.

오토런의 사례에서와 같이 결국, 내부망으로의 악성코드 감염을 사전억제하기 위해 내부망과 외부망에서의 이동식 매체 반·출입 정책을 명확히 규정할 필요가 있다. 또한, 내부망에서의 이동식 매체 사용을 가능한 자제하고, 해당 악성코드에 맞는 전용백신을 활용한 주기적인 검사를 병행해야 한다.

4.4 스마트폰용 악성코드로부터 정보유출 차단

BYOD 문화가 정착되고, 여러 가지 주요정보유출 가능성이 증가하는 실정이므로, 어플리케이션 다운로드를 설치하는 경우 신뢰되는 사이트에서 배포하는 어플리케이션만을 설치할 필요가 있다[15]. 2016년 7월부터 스마트폰의 개인정보만을 빼내던 기존버전에서 나아가 통화기능까지 제한하는 소위 '페이크뱅크.B (Android.Fakebank.B)' 라는 변종악성코드가 등장했다[26]. 해당 악성코드는 정보유출피해자가 본인이 소지하고 있던 정보가 유출되었다는 깨닫고 스마트폰으로 고객센터 혹은 형사사법기관에 신고를 위해 전화를 걸면 연결을 차단·방해하는 특징이 있다[3]. 피싱피해자는 전자 우편이나 다른 일반전화 등 다른 방법으로 해당기관에 신고해야 하고 반대로 해커는 개인정보를 충분히 훔칠 시간적 여유를 가지게 된다. 결국, 중요한 정보가 저장되어 있을 경우 암호화 어플리케이션을 활용하면 정보보호율이 기존보다 30% 이상 증가하는[5] 것으로 나타나므로 중요정보에 대한 암호화가 능동적으로 이루어져야 한다. 그리고 스마트폰 및 소프트웨어 백신을 최신 상태로 업데이트하고 악성행위 감시 어플리케이션을 활용하여 악성코드로부터 스마트폰을 안전하게 보호하여야 한다.

5. 결 론

이 논문은 국가안보측면에서 공공기관의 정보보안 시스템 현황 및 실태분석을 통해 예방대책을 제시하는 것이다. 공공기관에서 내부자에 의한 정보유출을 예방하기 위해서는 기술적 측면의 정보보안기술과 물리적 보안개념을 도입한 융합보안(Convergence Security)적 접근이 반드시 필요하다. 기술적 보안은 IT부서 또는 정보보호부서에서 담당하고, 물리적 보안은 안전부서 등에서 담당할 필요가 있다. 결론적으로, 정보보안의 데이터와 물리보안의 출입관리정보, CCTV 정보 등을 통합관리하면 종합적인 상황판단이 가능해지므로 이를 통해 내부정보 유출 시도를 사전에 차단할 수 있는 기회가 증가할 것이다[21].

그리고 내부정보 유출예방을 위해 모든 임직원들을 대상으로 인식 제고목적을 위한 교육 및 홍보가 우선적으로 이루어질 필요가 있다[23]. 최신 기술의 보안시스템을 선제적으로 도입하여도 조직의 임직원들의 보안의식이 낮으면 정보유출을 예방하는 것은 정말 어려운 일이다. 그러므로 핵심 인력에 대한 적절한 보상과 퇴직자들을 대상으로 한 체계적 관리 및 보안교육은 반드시 이루어져야 하며 이를 통해 보안정책 프로세스와 보안문화를 정착시켜야 한다.

또한, 내부정보유출방지를 위해 규정, 지침, 관리매뉴얼, 해당 관리조직 신설이 필요하다. 규정 및 지침을 통해 관리매뉴얼을 작성하여 내부정보 유출관련 실태파악을 하고 이에 상응하는 억제정책을 만들어야 한다. 그리고 관리조직을 통해 기업은 현재의 보안상황을 확인하여 문제점을 파악하고 정보 유출 발생 그리고 대응을 위한 체계를 마련할 필요가 있다.

마지막으로, 보안USB의 반출·입승인 절차 프로세스를 자동화할 필요가 있고 보안에 대한 인식전환이 반드시 필요하다. 관리자는 보안 관리는 비용효과를 증가시킨다는 인식을 바꾸고, IT 예산 확보를 통해 조직에 최적화된 보안 시스템 구축이 이루어져야 하며, 이를 관리하는 보안담당자에 의한 지속적인 모니터링 및 철저한 관리 감독이 이루어질 때 내부자에 의해 발생하는 정보유출문제를 예방 및 억제할 수 있다.

참고문헌

[1] 국세청, '정보보안 업무규정', 국세청, 2015.
[2] 국가정보원, 미래창조과학부, '2014 국가정보보호백서', 국가정보원, 2014.

[3] 김선주, “스마트폰 고유정보를 통한 안전한 개인키 관리 방안”, 콘텐츠학회논문지, 16(8), pp. 90-96, 2016.
[4] 김청하, 박석, “협업 필터링을 응용한 소셜 네트워크 서비스에서 프라이버시 유출 탐지 기법”, 정보과학회논문지: 데이터베이스, 40(3), pp. 168-178, 2013.
[5] 배기태, 정민영, “통신 호 네트워크 구간 암호화를 통한 스마트폰 통신 보안 전송 기법”, 컴퓨터정보학회발표논문집, 24(1), pp. 315-317, 2016.
[6] 이광우, 김승주, “기업 비밀정보 유출 방지 및 보호 관점에서의 디지털 복합기 보안 기술 동향 분석”, 정보보호학회지, 20(1), pp. 47-55, 2010.
[7] 이대성, “네트워크 바이오 인증 기반 산업기술 유출방지 연구”, 융합보안논문지, 11(4), pp. 31-36, 2011.
[8] 이창무, 김민지, ‘산업보안이론’, 법문사, 2013.
[9] 이창훈, 하옥현, “기밀유출방지를 위한 융합보안 관리 체계”, 융합보안논문지, 10(4), 61-67, 2010.
[10] 이희선, “기술유출범죄의 실태분석 및 대응방안 연구”, 민간경비학회보, 11(2), pp. 283-301, 2012.
[11] 안준선, 이은영, 창병모, “SW 개발보안을 위한 보안약점 표준목록 연구”, 정보보호학회지, 25(1), pp. 7-11, 2015.
[12] 정병일, “기업의 산업기술 유출방지 연구”, 산업보안연구학회논문지, 1(1), pp. 1-19, 2009.
[13] 장은겸, 이상준, 이중인, “파일 DNA 기반의 변종 악성코드 탐지를 위한 유사도 비교 연구”, 컴퓨터정보학회논문지, 19(1), pp. 85-94, 2014..
[14] 최관, “산업보안기밀 유출원인 연구”, 한국산업보안연구, 5(1), pp. 71-93, 2015.
[15] 최관, 김민지, “조선기업출입보안관리 발전을 위한 연구: 융합보안적 접근”, 한국시큐리티융합경영학회지, 4(2), pp. 187-202, 2015.
[16] 최판암, 이민형, “로지스틱 회귀분석을 통한 산업기밀유출방지에 영향을 미치는 기업보안 활동연구”, 민간경비학회보, 12(3), pp. 182-206, 2013.
[17] 최형규, ‘의심행위 및 악성링크 추적을 이용한 내부자료 유출 방지시스템 설계’, 한세대학교 일반대학원 박사학위논문, 2014.
[18] 채정우, 고영희, “전문경영인의 기업정보 보호를 위한 산업기술 유출요인과 대응전략에 대한 연구”, 전문경영인연구, 15(1), pp. 87-113, 2012.
[19] Betzer, A. & Theissen, E., “Insider Trading and Corporate Governance: The Case of Germany”, European Financial Management, 15(2), pp. 402-429, 2009.
[20] Cornish, B. D. & Clarke, R. V., ‘The Reasoning Criminal: Rational Choice Perspectives on Offending’, New Jersey, Springer-Verlag, 2014.
[21] Cziraki, P., Goeij, P. D. & Renneboog, L., “Corporate Governance Rules and Insider Trading Profits”, Review of Finance, 18(1), pp. 67-108, 2014.
[22] Gilbert, A. & Tourani-Rad, A., “The Impact of Regulations on the Informational Basis of Insider Trading”, Journal of Management, 33(2), pp. 407-435, 2008.
[23] Sizs, R. W. & Whidbee, D. A., “Insider Trades and Demand by Institutional and Individual Investors”, Review of Financial Studies, 23(4), pp. 1544-1595, 2010.
[24] 보안뉴스, 올해 상반기, 커뮤니티 사이트 통한 악성코드 유포‘성행’., 2016년 7월 17일자.
[25] 서울경제신문, 변종 스마트폰 ‘악성코드’, 카드정보 유출 신고까지 막는다., 2016년 7월 18일자.
[26] http://www.etnews.com/20160421000340 [2016.10.01. 검색].

[著者紹介]

최 관 (Kwan Choi)

호주 국립 모나쉬대학교
범죄학·형사사법학 박사
前) 한세대학교 인문사회학부 교수
現) 삼성교통안전연구소
책임연구위원
(산업보안업무 담당)

email : schgosi@daum.net

김 민 지 (Minchi Kim)

미국 뉴욕시립대학교 법심리학 박사
한국형사정책연구원 부연구위원
現) 숙명여자대학교 사회심리학과
교수

email : mkim76@sm.ac.kr