산업기밀 손실 방지를 위한 순환적 산업보안 관리과정 모델 구축에 대한 연구

Study on Building Cyclical Industrial Security Management Process Model for Industrial Secrets Loss Prevention

채정우* · 정진홍**

Jeong Woo, Chae · Jin Hong, Jeong

Abstract

This study is aims to present cyclical industrial security management process model as a non-financial risk management tool. First, the security management process of the international information security management certification system ISO/IEC 27001, KISA(Korea Internet & Security Agency) ISMS(Information Security Management System), PIMS(Personal Information Management System) were compared with their control items. The circulation system improvements are discussed. Based on this, 'industrial secrets life cycle', 'BORaI(Building, Operating, Reviewing and Improvement) cycle' and controls of each cycle are derived. Industrial security professionals verify the validity by Delphi surveys conducted over two times. Completed industrial security management process model consists of three cycles (Industrial secrets life cycle, BORaI cycle, and Industrial secrets infringement risk management process). 'Industrial secrets life cycle' is consist of industrial secrets creation, utilization, disposal stages. 'BORaI cycle' is consist of industrial security policy building, policy operating, operation review, improvement stages. Each step will be implemented sequentially with the positive(+) reflux.

Key words : Industrial security, Management process, Industrial espionage, ISMS, Technology leakage, PDCA, BORaI

요 지

본 연구는 비재무적 리스크 관리를 위한 순환적 산업보안 관리과정 모델을 제시할 목적으로 수행되었다. 먼저, ISO/IEC 27001, KISA(한국인터넷진흥원)의 ISMS, PIMS의 관리과정 통제항목들을 비교하고 순환체계 관련 연구들을 고찰하였다. 이를 토대로 '산업기밀 생명주기', 'BORaI 순환주기'를 도출하였다. 타당성 검증을 위해 산업보안전문가들을 대상으로 2차례의 델파이 조사를 하였다. 이에 따라 완성된 모델은 '산업기밀 생명주기', 'BORaI 순환주기', '산업기밀침해 위험관리 프로세스' 등 세 가지 순환주기로 구성되었다. '산업기밀 생명주기'는 산업기밀의 생성, 활용, 폐기 등 3단계로 구성된다. 'BORaI 순환주기'는 산업보안 관리과정의 메인 사이클로서 산업보안정책 구축, 정책 운영, 운영 검토 및 개선 등 3단계로 구성되며 순차적 단계 이행으로 긍정적인(+) 환류가 지속되는 것이다.

핵심용어 : 산업보안, 관리과정, 산업스파이, 정보보호관리체계, 기술유출, PDCA, BORaI

1. 서 론

지속적인 세계 금융위기로 우리 기업들은 치열한 국제 비즈니스 환경에서 생존하기 위해 첨단 과학기술력의 제고와 지식재산권 보호에 사활을 걸고 있으며, 이는 국가경쟁력을 좌우하는 중요한 요인이 되고 있다. 이를 뒷받침하기 위해 우리나라는 국가정보원이 2003년에 산업기밀보호센터를 설치하여 산업보안활동을 본격적으로 전개하여 왔다. 이후로 기존

의 정보기술 중심의 보안에서 기업경영전략과 연계되어 포괄적·융합적으로 접근하는 산업보안 전문인력 양성 교육기관과 연구들이 출현하기 시작하였다. 그러나 산업기밀이라는 연구대상의 특성상 정보원에 대한 심층적인 접근과 공개가 어려워 일반적인 정보보안 분야에 비해 학문적 인식과 관심이 미약하였다. 특히, 산업보안 분야는 아직 독자적인 공인 인증체계가 정립되어 있지 않아 실무상으로도 산업보안활동을 총체적(holistic) 관점에서 관리하기 위한 공용(共用)의 준거 프

*정회원. 서울과학종합대학원대학교 경영학 박사수료, 산업보안 전공(E-mail: wiseguy21@naver.com)

Member. Ph.D Candidate, Department of Business administration, aSSIST

**교신저자. 정회원, 서울과학종합대학원대학교 교수, 산업정보대학원장(Tel: +82-070-7012-2743, Fax: +82-2-360-0796, E-mail: jhjeong@assist.ac.kr)

Corresponding Author. Member. Professor, aSSIST

레이워크가 없는 실정이다. 이와 달리, 정보보안 분야의 경우 국제 인증체계인 ISO/IEC 27000시리즈를 통해 통신·의료·금융과 보험 등 산업별, 통제영역별 세분화된 표준체계들이 제정되어 가는 추세이다(지식경제부, 2010). 따라서 본 연구에서는 국제 정보보안경영인증체계인 ISO/IEC 27001과 국내 인증체계인 KISA의 ISMS, PIMS의 관리과정 모델과 통제항목들을 비교·분석하고, 순환적 관리시스템 개선과 산업보안에 관한 선행연구들을 고찰하여 산업보안에 적합한 관리과정 모델을 탐색적으로 도출하고자 한다. 모든 분야의 산업자산 보호와 손실예방까지 고려한다면 연구범위가 과도하게 확대되므로 본 연구에서의 제안모델은 국내 산업보안 관련 법령에 근거하여 영업비밀의 보호, 산업기술·국가핵심기술 유출방지, 전략물자·전략기술 관리 등을 대상으로 하여 논한다.

2. 이론적 배경

2.1 순환적 시스템 개선 운영모델로서의 PDCA

PDCA(또는 PDSA) 모델은 일반적으로 Deming Cycle이라고도 하며, Deming의 수레바퀴, 지속적인 나선형 개선(Continuous Improvement Spiral) 등으로도 알려져 있다. 지속적인 개선 및 학습을 위한 계획(Plan), 실행(Do), 확인(Check or Study), 조치(Act)로 구성된 반복적인 단계를 논리적 순서로 연결한 것이다. 1920년대에 계획(Plan), 실행(Do), 평가(See)의 개념을 도입한 통계전문가 Walter A. Shewhart에 의해 착안되었고 Shewhart의 Cycle을 W. Edwards Deming은 위와 같이 네 단계로 변형, 발전시켰다. 핵심 개념은 Fig. 1과 같이 순환을 반복함으로써 목표가 달성될 때까지 계획과 실천 방식을 끊임없이 개선해 나가는 것이다. 계획(Plan)단계는 변화를 위한 사전 작업으로 결과 분석 및 예측을 하는 것이며, 실행(Do)단계는 통제된 상황에서 조치를 취하면서 계획을 실행하고, 확인(Check)단계는 결과를 연구하거나 재검토하는 것이고, 조치(Act)단계는 프로세스를 표준화하거나 개선하기 위한 행동을 행하는 것이다. PDCA 모델의 이점으로는 개인과 팀의 일상적인 관리, 문제 해결과정, 프로젝트 관리, 지속적인 개선, 벤더(vendor)개발, 인적자원 개발, 신제품 개발, 프로세스 시험(Process trials)에 탁월하다는 것이며¹⁾,

Fig. 1. PDCA circular model (source: <http://en.wikipedia.org/wiki/PDCA>)

¹⁾<http://asq.org/learn-about-quality/project-planning-tools/overview/pdca-cycle.html>

Kaizen(개선기법)과 Just-in-time(JIT, 적시생산시스템)등의 운용과 관련이 있다(최흥기, 2009). 이러한 PDCA 모델은 제품 품질이나 생산성 향상 등 전통적인 활용분야 뿐만 아니라 과학적 문제해결방법의 하나로 다양하게 응용되고 있다. 먼저, 신승호 외(2007)는 PDCA 모델을 적용한 연구를 조직성과 증진 측면과 단계별 세부 활동 측면으로 구분하면서 단계별 적용 사례 연구로 행정정보화의 위험관리, BSC 구축, 리엔지 리어링, 성과관리효과 극대화 모형 등이 있다고 하였다. 박승욱 외(2010)의 경우, 광범위하고 복잡한 절차의 특성을 가지는 국가 R&D 관리제도의 현황 파악을 위해 PDCA 모델을 기반으로 국가 R&D 관리 프로세스의 R&D 계획 범위를 정의하였다. 장종기 외(2011)는 CMMI-DEV의 RSKM 프로세스와 PMBOK의 위험관리 지식영역의 개별 프로세스를 PDCA 모델 기반으로 병합하여 기존 프로세스 보다 개선된 IT 프로젝트 위험관리 프로세스를 설계·구현하였다. 특히 정보보호 분야의 적용 사례를 보면, 정창화 외(2011)는 항공기 반시설용 정보보호 관리체계 모델을 제안하면서 그 보안성 평가에는 계획(Plan), 활동(Do), 평가(Check), 조치(Action)업무로 이어지는 생명주기(Life Cycle) 구조가 지속적으로 개선되는 순환적 프레임워크 구조를 가져야 한다고 하였다. 한국 정보보호진흥원(2007)도 개인정보보호 수준지표의 구성요소 정립을 위해 개인정보를 PDCA 모델과 라이프사이클 관점에서 분석할 필요가 있다는 전제하에, 계획(Plan) 단계는 실시(Do) 단계의 실행근거로서 개인정보보호에 대한 정책이나 계획을 수립하고, 실시(Do) 단계는 개인정보보호를 위한 투입과 활동으로 구분되며, 평가(Check) 단계는 개인정보보호 정책 등의 수립과 이에 의한 시행을 평가하는 것이고, 개선(Act) 단계는 평가(Check)단계에서의 평가를 기반으로 계획(Plan)단계로의 피드백을 통해 차후의 개인정보보호 정책 등의 수립에 반영시키는 단계로 보았다.

2.2 ISO/IEC 27001과 K-ISMS의 관리과정

2.2.1 ISO/IEC 27001의 관리과정

IT보안 관련 표준은 크게 국제표준과 산업표준으로 나뉘는데 약 200종 이상의 표준이 존재하고 있다(금융보안연구원, 2009). 그 중 ISO/IEC JTC1/SC27에서 제정한 ISO/IEC 27001은 대표적인 정보보안경영인증체계 국제표준으로 ISMS(Information Security Management System)의 수립, 설계, 운영, 감시, 검토, 유지 및 개선을 통한 조직의 정보보호 강화를 목적으로 하고 있다. ISO/IEC 27001은 1998년에 제정된 BS7799 part2를 바탕으로 2005년 10월에 국제표준으로 제정되었으며, 우리나라를 비롯하여 미국, 영국, 인도, 일본, 대만 등 전 세계 많은 조직들에서 활용되고 있다. 2012년 10월 현재 인증을 취득한 조직의 수는 7,940개 이다. 특히 일본에서는 그 인식과 활용도가 높아 4,100여개의 인증이 발급되었다²⁾. 또한 전체 구조가 품질경영인증표준(ISO 9001:2000)과 환경경영인증표준(ISO 14001:2004)과 대비될 수 있기 때문에 기존의 기업경영체계에 통합하여 운영할 수

²⁾<http://www.iso27001certificates.com/>

있다. ISO/IEC 27001에서는 ISMS 구축을 위한 필수 요구사항들을 기술하고 있으며, 규모에 관계없이 모든 유형의 조직들에 적용된다. 부록 A는 정보보호 관리를 위한 총133개의 정보보호 통제사항을 담고 있다. 정보보호 관리업무를 경영진 통제 하에 두는 것은 지속가능하고, 지도되면서 지속적인 향상을 위한 선결조건이다. 따라서, ISO/IEC 27001는 일회성의 정보보호 활동이 아닌 새로운 보안 위협과 취약점들, 정보보호 실패로 인한 영향 등을 지속적으로 검토하고 주의 깊게 그 변화를 주시하면서 이에 적응하기 위한 경영시스템으로서 프로세스 접근관점으로 구성되어 있다. 이를 위해 PDCA 모델을 채택하였는데, 정보시스템과 네트워크 보안을 위한 OECD 가이드라인 원칙들이 반영되었다. Fig. 2는 입력으로서의 정보보호 요구사항과 기대가 어떻게 이해관계자들을 만족시키는 보안관리의 결과물로 출력되는지 전체적인 ISMS 관리과정을 보여주고 있다. 각 단계별 통제사항은 다음과 같다(ISO/IEC, 2005a, b).

① Plan (ISMS의 수립)

- 1) ISMS의 범위와 경계를 정의한다.
- 2) ISMS의 정책을 정의한다.
- 3) 조직의 위험평가 접근을 정의한다.
- 4) 위험을 식별한다.
- 5) 위험을 분석하고 평가한다.
- 6) 위험 처리를 위한 옵션들(수용, 처리, 회피, 전가 등)을 파악하고 평가한다.
- 7) 위험 처리를 위한 통제목표들과 통제사항들을 선택한다.
- 8) 제시된 잔여 위험에 대한 경영진의 승인을 얻는다.
- 9) ISMS를 수행하고 운영할 수 있도록 경영진의 권한 부여를 획득한다.
- 10) 적용 명세서(Statement of Applicability)를 준비한다.

② Do (ISMS의 실행과 운영)

- 1) 위험 처리 계획을 세운다.
- 2) 파악된 통제목표를 달성하기 위한 위험 처리 계획을 실행한다.
- 3) 통제목표를 충족하기 위해 선택된 통제사항들이나 그 그룹들을 실행한다.
- 4) 선택된 통제사항들의 효과성을 측정하는 방법을 정의하고, 측정결과물들이 통제 효과성을 평가하는데 어떻게 사용될 것인지 기술한다.
- 5) 훈련과 인식 제고 프로그램들을 실행한다.
- 6) ISMS의 운영을 관리한다.
- 7) ISMS의 운영을 위한 자원들을 관리한다.
- 8) 즉각적인 보안 이벤트의 감지와 보안 사고에 대응할 수 있는 절차들과 그 밖의 다른 통제사항들을 실행한다.

③ Check (ISMS의 감시와 점검)

- 1) 감시를 시행하고, 절차들과 통제사항들을 점검한다.
- 2) 보안감사 결과, 사건, 효과성 측정결과물, 제안, 이해관계자들로부터의 피드백 등을 고려하여 정기적인 ISMS의 효과성 검토를 수행한다.
- 3) 보안 요구사항들이 만족되고 있는지 확인하는 통제사항들의 효과성을 측정한다.

Fig. 2. PDCA model applied to ISMS processes (source: ISO/IEC 27001)

- 4) 계획된 주기마다 위험평가와 잔여위험을 검토하고 수용 가능한 위험수준을 파악한다.
- 5) 계획된 주기마다 내부 ISMS 감사를 실시한다.
- 6) ISMS에 대한 범위가 적절한지와 절차의 개선이 파악되었는지 규칙적으로 경영진의 검토를 수행한다.
- 7) 감시와 점검의 결과를 고려하여 보안 계획을 갱신한다.
- 8) ISMS의 효과성이나 성과에 영향을 줄 수 있는 행위나 이벤트를 기록한다.

④ Act (ISMS의 유지, 개선)

- 1) ISMS에서 파악된 개선사항들을 실행한다.
- 2) 적절한 교정과 예방조치를 취하며, 조직 내 그리고 타 조직의 보안 경험을 적용한다.
- 3) 주변 환경에 관련하여 구체적으로 적합한 수준으로 모든 이해 관계자들에게 조치와 개선사항에 대해 알리고, 어떻게 진행할지 동의를 구한다.
- 4) 의도한 통제목표를 달성하기 위한 개선사항들을 실행할 수 있도록 한다.

2.2.2 K-ISMS의 관리과정

K-ISMS는 2002년에 구(舊) 정보통신부와 한국인터넷진흥원(KISA)이 정보통신사업자의 보안성 강화를 위해 개발한 정보보호 프레임워크로서, 2006년 12월에는 한국정보통신기술협회(TTA)의 표준으로도 채택되었으며, 2008년 5월에 방송통신위원회가 인증에 대한 고시를 하였다(방송통신위원회, 2011). K-ISMS는 ISO/IEC 27001과 같은 국제표준을 수용하면서도 국내 상황에 적합하게 설계된 보안관리 표준모델이다. K-ISMS는 Fig. 3과 같은 5단계 관리과정(총14개 통제항

Fig. 3. K-ISMS management circle (source: KISA)

목), 문서화(총3개 통제항목), 그리고 15개의 보안통제영역(총 120개 통제항목)으로 구성되어 있다. 인증을 받기 위해서는 첫째, 5단계 정보보호 관리과정에 따라 해당 조직의 ISMS를 수립하고 운영해야 하고, 둘째, ISMS 수립 및 운영에 관한 사항을 문서화해서 관련자들이 쉽게 이용할 수 있도록 해야 하고, 마지막으로 위험분석을 통해 필요한 통제사항을 선정하여 이에 해당하는 정보보호대책을 구현·운영해야 한다. 이중 가장 기반이 되는 “정보보호 관리과정”과 “문서화”의 통제항목들은 K-ISMS 인증 심사시 15개 보안통제영역의 통제사항들과 달리 선택사항인 아닌 필수사항이다. K-ISMS는 조직의 전반적인 비즈니스 활동과 위험이 잠재된 대내외 환경에서의 정보보호를 목적으로 하므로 “정보보호 관리과정”을 통해 수립되어지며, 보호대상 자산과 위험관리를 위한 접근방법, 통제사항, 조직이 요구하는 보증 정도(수준)를 포함한다. 즉, ISMS의 이행을 위해 조직은 ① 정보보호정책 수립, ② ISMS 범위설정, ③ 위험관리, ④ 구현, ⑤ 사후관리로 구성된 5단계의 논리적, 체계적인 정보보호관리 프레임워크를 기획·수립 및 관리하게 되는 것이다.

K-ISMS의 “정보보호 관리과정” 14개 통제사항들은 각 단계별로 다음과 같다.

① 정보보호정책 수립 (총2개)

- 1) 정보보호정책의 수립
- 2) 조직 및 책임의 설정

② ISMS 범위설정 (총2개)

- 1) ISMS 범위설정
- 2) 정보자산의 식별

③ 위험관리 (총5개)

- 1) 위험관리전략 및 계획 수립
- 2) 위험분석 3) 위험평가
- 4) 정보보호대책 선택
- 5) 정보보호계획 수립

④ 구현 (총2개)

- 1) 정보보호대책의 효과적 구현
- 2) 정보보호 교육 및 훈련

⑤ 사후관리 (총3개)

- 1) ISMS의 재검토
- 2) ISMS의 모니터링 및 개선
- 3) 내부감사

2.3 PIMS의 관리과정

PIMS는 방송통신위원회와 KISA가 기업이 고객에 대한 개인정보보호 활동을 체계적·지속적으로 수행할 수 있도록 2010년에 개발한 개인정보보호 프레임워크이다(방송통신위원회, 2011). PIMS는 K-ISMS, ISO/IEC 27001, BS10012 등 국내외 정보보호표준과 정보통신망 이용촉진 및 정보보호 등에 관한 법률에 명시된 개인정보보호조치를 고려하여 국내 환경에 적합하게 보완하여 개발된 것이다. 다른 ISMS에 비해 개인정보 관련 컴플라이언스(Compliance)에 대응하기 위한 보안대책 구현사항과 법적 준거성, 전반적인 체계운영 측면이 강조되었다. 즉, ISO/IEC 27001과 K-ISMS가 정보보호

Fig. 4. PIMS management circle and personal information life cycle (source: KISA)

전반에 걸쳐 일반적으로 적용될 수 있는 정보보호 요구사항으로 구성되어 있는 반면, PIMS는 그뿐만 아니라 개인정보 보호의 법률적 기준을 추가하고 개인정보의 생명주기(수집, 이용, 보유, 제공, 파기 등)를 모두 반영하여 개인정보보호 활동을 체계적, 효과적으로 관리할 수 있게 하고 있다. PIMS는 Fig. 4와 같은 5단계 개인정보보호 관리과정(총11개 통제항목)과 3단계 개인정보 생명주기(총28개 통제항목), 그리고 9개의 보안통제영역(총79개 통제항목)으로 구성되어 있다. “개인정보보호 관리과정”의 경우 K-ISMS와 단계 구분은 거의 유사하나 통제항목수가 각 단계별로 상이하며 전체적으로는 3개 항목이 적다. 그 대신 “개인정보 생명주기”를 PIMS에 추가로 편입하여 개인정보의 수집부터 폐기까지에 대한 구체적인 보호조치들을 규정하고 있다.

PIMS의 “개인정보보호 관리과정” 11개 통제사항들은 각 단계별로 다음과 같다.

① 개인정보 정책 수립 (총3개)

- 1) 개인정보보호정책 수립
- 2) 조직 및 책임 설정
- 3) 내부 관리계획의 수립

② PIMS 범위설정 (총2개)

- 1) 개인정보 식별
- 2) PIMS 범위 설정

③ 위험관리 (총3개)

- 1) 위험관리 계획 수립
- 2) 위험평가
- 3) 위험관리를 위한 보호대책 및 이행계획 수립

④ 구현 (총1개)

- 1) 개인정보보호 대책의 이행계획에 따라 보호대책을 구현하고, 이후 검토계획에 따라 일정 시간이 경과한 후 그 성과를 검토, 보고한다.

⑤ 사후관리 (총2개)

- 1) 모니터링 및 개선
- 2) PIMS의 재검토

PIMS의 “개인정보 생명주기”는 개인정보 취급 생명주기와 관련된 법적 요구사항을 각 단계별로 구분하여 각각에 대한 구체적인 실행방법을 명시하고 있다. 28개 통제사항들은 다음과 같다.

① 개인정보 수집 (총7개)

- 1) 서비스 제공을 위해 필요한 최소한의 정보수집
- 2) 중요 정보 수집 제한
- 3) 간접 수집시 조치
- 4) 정보주체의 동의
- 5) 법정대리인 동의 획득 및 고지
- 6) 동의 기록 보관
- 7) 개인정보 취급 방침

② 개인정보 이용 및 제공 (총16개)

- 1) 목적 내 개인정보 이용
- 2) 이용자의 불만 처리
- 3) 열람정정요구권 보장 및 처리
- 4) 동의 철회
- 5) 이용자 요청의 처리
- 6) 이용자 고지 및 동의
- 7) 위탁자 책임
- 8) 외부 위탁관리 감독
- 9) 외부 위탁계약 관련사항
- 10) 제3자 제공시 동의
- 11) 제공받은 개인정보의 관리
- 12) 제3자 보안관리
- 13) 제3자 제공시 계약 관련사항
- 14) 개인정보를 이전하는 경우 보호조치
- 15) 개인정보를 이전받는 경우 보호조치
- 16) 해외 이전시 보호 조치

③ 개인정보 관리 및 폐기 (총5개)

- 1) 개인정보의 저장 및 관리
- 2) 파기규정
- 3) 파기시점
- 4) 파기방법
- 5) 목적 달성후 보유

2.4 보안관리에서의 순환적 관리과정에 대한 고찰

지금까지 살펴본 바와 같이 대부분의 정보보호관리 프레임워크는 PDCA 모델을 기반으로 하고 있으며, 프로세스 지향(process-oriented), 통제 기반(control-based), 측정 중심(measurement-driven)의 특징들을 공통적으로 가지고 있다. 이와 같은 프레임워크들은 정보보호와 개인정보보호를 단순히 기술적인 것으로만 보지 않고, 위험관리 기반의 관리·기술·물리적 통제들을 포함하는 전사 차원의 정보보호를 구현하기 위한 체계화된 일종의 경영시스템으로 간주되고 있다(금융보안연구원, 2011b). 실제로 앞서 살펴 본 ISMS들은 경영전략과의 연계를 강조하고 있으며, 전체 구조가 서로 유사한 부분이 많음을 알 수 있다. K-ISMS도 ISO/IEC 27001를 참조하여 개발되었고, 개인정보보호에 특화된 PIMS도 K-ISMS의 통제항목을 준용하여 수립되었으므로, K-ISMS에서 개인정보를 위주로 적용할 수 있어 정보보호와 개인정보보호를 완전히 구분하는 것은 어려움이 있다(금융보안연구원, 2011a). 산업기밀 보호를 목적으로 하는 산업보안관리체제도 이런 의미에서 기존 ISMS들과 겹치는 부분이 적지 않다고 볼 수 있기 때문에 기본 골격은 이들의 전체 구조와 비슷한

형태로 정립하여 상호 호환성과 운영성을 담보할 수 있어야 한다. 따라서 산업보안활동에서의 관리과정도 PDCA 사이클을 따르는 양(+)의 피드백 순환체계가 되어야 한다. 박인범 외(2011)도 산업보안문화형성을 위한 전반적인 보안정책관리를 PDCA 모델을 차용하여 설명하고 있다. 그러나 산업보안 관리과정이 PDCA 모형에 기초한다 하더라도 각 단계의 구성과 통제사항은 산업보안 고유의 특성이 반영되어야 한다. 기존 ISMS는 어떤 형태의 조직에도 적용 가능한 일반적, 범용적인 특징을 갖고 있어 보호 대상이 되는 정보 자체의 속성(기밀성, 무결성, 가용성 등) 손실 방지에 초점이 맞춰져 있다. 반면에 산업보안관리체계는 산업기술, 국가핵심기술, 영업비밀(기술·경영상 정보) 등과 같은 산업기밀을 보호하는 것을 주요 목적으로 한다. 그러므로 산업기밀을 활용하는 비즈니스 내용도 고려해야 한다. 또한 산업기밀은 조직목표와 대내외적인 사업환경 변화에 따라 영업비밀의 경우 생성과 폐기, 산업기술이나 국가핵심기술의 경우 지정과 해제가 거듭될 수 있으므로 PIMS의 개인정보 생명주기 관리과정처럼 산업기밀 생명주기에 맞춰 관리과정을 운용해야 한다. 즉, 기존 ISMS들의 기술적·물리환경적 보호기반하에 산업기밀침해 예방·관리부터 보안정책 운영의 검토·개선에 이르는 일련의 산업보안활동 프로세스에 대한 통제내용을 포함해야 한다. 이처럼 산업보안관리체계에 있어서의 관리과정은 조직화된 거버넌스(governance)의 한 축으로서 산업보안 정책 수립, 위험 식별, 위험 측정, 통제사항 개발과 실행, 관련 법령이나 규제 준수, 운영 평가, 지속적인 모니터링과 개선 등과 같이 PDCA 사이클에 따라서 구현되되 산업보안 특성과 산업기밀 보유 조직에 적합하도록 변환하여 설계되어야 한다.

3. 연구방법

3.1 델파이 기법 개요

델파이기법은 미국 RAND연구소에서 1953년에 최초로 시도되었다. 당시 의사결정에 도움을 받기 위해 선정된 자문집단에게 반복적이고 통제된 설문과정을 사용하였다. 전문가들의 의견을 수렴하여 미래를 예측하고, 정책대안을 탐색하는 방법에는 일반적으로 브레인스토밍(brainstorming)을 활용할 수 있다. 브레인스토밍은 자유로운 환경에서 가능한 많은 아이디어를 얻기 위한 방법이나, 외향적이고 공격적 성향의 참여자에 의한 발언기회의 독점, 공개적인 반대 의사 표시의 어려움 등의 약점이 있다. 델파이 기법은 이러한 단점을 극복하기 위한 연구방법으로 반복과 환류, 익명성, 합의, 통계적 표현 등의 특성을 가지고 있다(국토연구원, 2009).

3.2 조사대상

델파이 조사대상은 산업보안 관련 연구 및 실무분야의 전문가로서 교수, 보안관리자, 석사 이상 관련 연구자, 전문과정 수료자이다. 패널 선정에 있어 산업보안에 대한 전반적인 이해도와 식견을 주요 기준으로 삼았다. 즉, 본 연구의 델파이 패널은 다음 기준을 충족하는 전문가를 목적적 표집하여 설문대상자로 선정하였다.

Table 1. Demographic Profile of Delphi Panel

나이	빈도	백분율(%)	직위	빈도	백분율(%)
20대	1	3.7	대리 이하	5	18.5
30대	10	37.0	부장 이하	15	55.6
40대	12	44.4	임원 이상	4	14.8
50대 이상	4	14.9	교수	3	11.1
Total	27	100.0	Total	27	100.0
학력	빈도	백분율(%)	경력	빈도	백분율(%)
석사 이하	21	77.8	10년 이하	10	37.0
박사수료	2	7.4	20년 이하	12	44.4
박사	4	14.8	20년 초과	5	18.5
Total	27	100.0	Total	27	100.0

① 산업보안 관련 연구를 수행하였거나 교육경력이 있는 석사 이상의 자

② 기업 또는 기타 단체 등에서 관리적·기술적·물리적 보안업무를 수행하고 있는 자

이상과 같은 선정기준을 만족하는 전문가 중 참여 의사가 있는 총 27명의 산업보안 관련 전문가들로부터 의견을 수렴과 설문 평가를 받았다. 델파이 패널들의 인구통계적 분포는 Table 1과 같다.

3.3 연구절차 및 분석방법

우선 2장에서 살펴 본 ISMS들의 관리과정의 내용을 각 단계별로 비교하고 PDCA 모델에 대한 문헌 고찰을 통해 산업보안관리체계의 순환적 관리과정 모델인 ‘산업기밀 생명주기’와 ‘BORaI³⁾ 사이클’을 도출하였다. 통제사항의 내용은, 2장의 ISMS들의 관리과정과의 호환성을 보장하기 위해 오홍룡 외 3인(2005)의 ‘국내 정보보호 표준화 로드맵’과 그 외 공통사항들을 기본 골격으로 하여 ISMS들의 통제사항을 비교·검토하여 도출하였다. 이후, 1차 조사에서는 델파이 패널들에게 연구의 개요를 설명하고 개발된 관리과정 모델의 통제사항을 설문항목으로 만들었다. 설문 형태는, Likert 7점 평가 척도로 설문의 중요도를 평가하도록 한 폐쇄형과 설문 내용에 대해 자유롭게 의견을 개진할 수 있도록 개방형을 병행하였다. 1차 조사에 폐쇄형 설문을 사용한 이유는 기존의 공인 ISMS들과 내용적 일관성을 갖춰 산업보안관리체계 구성요소로서의 타당성을 높이는 동시에 패널들의 논의 초점을 집중시켜 연구 주제에 보다 합치하는 의견을 수렴하고자 함이었다. 1차 조사는 2012년 12월 22일부터 2013년 1월 5일까지 이메일로 설문을 배포하여 응답받는 형식으로 시행되었다. 수집된 자료는 SPSS 17.0을 이용하여 평균, 표준편차, 사분범위 등을 산출하였다. 2차 델파이 조사는 1차 조사와 동일한 방법으로 2013년 1월 7일부터 2013년 1월 17일까지 시행하였다. 1차 조사 결과에 따른 패널 의견을 반영하여 설문을 수정하였으며, 폐쇄형으로 각 설문의 중요도를 Likert 7

점 척도로 평가하도록 하였다. 이때 1차 조사에서의 분석결과를 피드백⁴⁾하여 설문에 대하여 재고 및 수정할 수 있게 하였다. 수집된 평가자료는 1차 조사 분석과 마찬가지로 기술적(descriptive) 통계처리를 하였으며, 조사결과의 타당성을 정밀하게 검증하기 위해 켄달(Kendall)의 W검증을 함께 실시하였다.

4. 조사결과 분석 및 산업보안 관리과정 모델 제안

4.1 조사결과 분석

2장의 이론적 논의와 2차에 걸친 델파이 조사결과를 바탕으로 ‘산업보안 관리과정 모델’을 도출하였다. 이는 ‘산업기밀 침해 위험관리 프로세스’를 포함하는 ‘BORaI 순환주기’와 ‘산업기밀 생명주기’로 구성된다. 순환주기의 구조나 통제항목 구성에 관해 패널들의 이의는 없었으며, 일부 통제사항의 설명에 대한 수정의견이 있어 이를 반영하였다⁵⁾. 먼저, ‘BORaI 순환주기’는 3단계의 11개 통제항목으로 구성된다.

① 산업보안정책 구축⁶⁾ (총6개)

- 1) 산업보안정책 수립
- 2) 담당조직 구성 및 책임·권한 설정 - 산업보안 활동에 대한 담당조직을 구성하고, 소요 인원과 예산을 분기/반기/연간 등 기간별로 명확히 (‘필요한 인원과 예산을’에서 문구 변경) 배정한다. 이때 활동을 수행, 검증하는 인력들에 대한 책임과 권한, 상호관계 설정 등 구성에 따른 운영계획도 수립하며 최고경영진의 승인과 지원을 보증 받는다.

- 3) 산업기밀 목록화
- 4) 침해위험 관리계획 수립
- 5) 침해위험 분석·평가
- 6) 침해위험 보호대책 수립

② 산업보안정책 운영 (총2개)

- 1) 산업기밀보호대책 구현
- 2) 산업보안 교육 및 훈련

③ 산업보안정책 운영 검토·개선 (총3개)

- 1) 모니터링 및 개선 2) 보안감사
- 3) 산업보안관리체계의 재검토

‘산업기밀 생명주기’는 3단계의 15개 통제사항으로 구성된다.

① 산업기밀 생성 (총4개)

- 1) 산업활동 성과물 권리화 또는 영업비밀 관리
- 2) 국가핵심기술의 관리
- 3) 생성단계 관련자 최초 보안교육 실시
- 4) 직무발명 보상

② 산업기밀 활용 (총8개)

- 1) 기술계약 체결시 관리 - 공동연구, 투자유치, 인수합병(M&A), 합작투자, 제조위탁, 라이선스 계약 등 기술계약

³⁾Building, Operating, Reviewing and Improvement등 3단계 산업보안관리 순환 사이클을 의미하는 영문 약어임.

⁴⁾설문항목마다 1차 조사시의 평균과 표준편차를 제시함.

⁵⁾통제항목 내용 설명부분에 밑줄 처리된 부분임.

⁶⁾통제항목 4), 5), 6)번은 ‘침해위험관리 프로세스’임.

을 체결할 시에는 상대방과 비밀유지계약을 별도로 체결하며 분쟁해결방법을 명시한다. 이와 더불어 보안교육을 실시하여 상호 보안준수사항을 인지하도록 한다. (내용 추가)

- 2) 국가핵심기술의 수출시 관리
- 3) 전략기술 · 전략물자의 수출시 관리
- 4) 산업기밀관리 외부 위탁
- 5) 제3자 제공시 관리
- 6) 제공받은 산업기밀의 보호
- 7) 이전 또는 이전받은 산업기밀의 보호
- 8) 산업기밀 해외 이전시 보호
- ③ 산업기밀 파기 (총3개)
 - 1) 파기규정 수립
 - 2) 파기시점 - 산업기밀의 활용목적이 달성되었거나 경제적 가치 상실 등의 사유 발생시에는 경영진의 판단에 따라 보존하거나 파기하되, 후자의 경우 (‘가치 상실 등 파기 사유가 발생한 경우에는’에서 문구 변경) 산업기밀이 저장된 매체, 문서 등은 지체 없이 파기한다.
 - 3) 파기방법

위와 같은 통제항목으로 설문한 ‘BORal 순환주기’에 대한 조사결과는 다음과 같다. 먼저, 켄달의 W검증 결과는 Table 2에서 보는 바와 같이 1, 2차 조사 모두 유의확률이 .000으로 $p < .05$ 에 해당되어 통계적으로 유의한 모델로 입증되었다. 따라서 제안된 ‘BORal 순환주기’는 패널들의 합의가 형성된 사이클로 판명되었다. 켄달의 일치도 계수 W는 1차 조사에서 .138이었으나 2차 조사에서 .191로 높아져 패널의견 수렴

Table 2. ‘BORal Cycle’ Verification Result

Statistics	Round 1	Round 2
Kendall's W ^a	.138	.191
Chi-Square	37.199	34.322
df	10	10
Asymp.Sig.	.000	.000

^aKendall's Coefficient of Concordance

Table 3. ‘BORal Cycle’ Controls Analysis Result

순환주기 단계	통제항목	Round 2 Statistics		
		Mean	S.D.	M.R.
산업보안 정책 구축	담당조직 구성 및 책임 · 권한설정	6.3889	.77754	7.44
	산업보안정책 수립	6.4444	.61570	7.69
	산업기밀 목록화	5.7778	.64676	4.64
	침해위험 관리계획 수립	6.0556	.53930	5.92
	침해위험 분석 · 평가	6.1111	.47140	6.08
	침해위험 보호대책 수립	6.0556	.41618	5.75
산업보안 정책 운영	산업기밀 보호대책 구현	6.0556	.63914	5.92
	산업보안 교육 및 훈련	6.2778	.89479	6.92
산업보안 정책 운영 검토 · 개선	모니터링 및 개선	6.1111	.75840	6.22
	보안감사	6.0000	.68599	5.53
	산업보안관리체계의 재검토	5.5556	.70479	3.89

Table 4. ‘Industrial secrets life cycle’ Verification Result

Statistics	Round 1	Round 2
Kendall's W ^a	.091	.163
Chi-Square	34.433	41.071
df	14	14
Asymp.Sig.	.002	.000

^aKendall's Coefficient of Concordance

정도가 향상됨을 보이므로 델파이 조사 목적에 부합하였다. Table 3은 각 항목별 기술적 통계값인 평균(Mean), 표준편차(S.D.), 평균순위(M.R.)를 나타내고 있다. 단순히 최종 2차 조사결과와 기술통계치만 감안하더라도 모든 항목이 Likert 7점 척도 중 평균 5.5점을 초과하고, 표준편차도 1이하로 나타나 패널의 합의 정도가 높으므로 순환주기를 구성하는 통제항목으로써 타당함을 보여준다. 본 순환주기에서는 ‘산업보안정책 수립’ 항목이 최종 조사에서 평균 6.4444점을 얻어 가장 높은 중요도를 보였다. 반면 ‘산업보안관리체계의 재검토’ 항목은 5.5556점을 얻어 상대적으로 낮게 평가되었는데, 산업기밀의 보호는 관리시스템 구축 초기에 정교한 보안정책을 수립하여 시행하는 것이 사후 개선, 검토보다 더 중요함을 보여주고 있다.

‘산업기밀 생명주기’에 대한 조사결과를 살펴보면 다음과 같다. Table 4. 켄달의 W검증 결과를 보면, 1차는 유의확률이 .002이고, 2차는 .000으로서 $p < .05$ 에 해당되어 모두 통계적으로 유의하였다. 따라서 제안된 ‘산업기밀 생명주기’는 전문가들의 합의가 도출된 사이클로 판명되었다. 켄달의 일치도 계수 W는 1차 조사에서는 .091이었고, 2차 조사에서는 .163으로 더 높아져 패널의견 수렴정도가 향상되었기 때문에 델파이 조사 목적에 부합하였다. Table 5에서 2차 조사결과와 기술통계치를 보면 모든 항목이 Likert 7점 척도 중 평균(Mean) 5.7점을 초과하였으며, 표준편차(S.D.)도 1이하이므로 생명주기를 구성하는 통제항목으로서 유의미함을 보여준다. 본 생명주기에서는 ‘산업활동 성과물 권리화 또는 영업비밀 관리’ 항목이 최종 조사에서 평균 6.5000점을 얻어 가장 높은 중요도를 보였고, ‘직무발명 보상’ 항목은 5.7222점을 얻

Table 5. 'Industrial secrets life cycle' Controls Analysis Result

생명주기 단계	통제항목	Round 2 Statistics		
		Mean	S.D.	M.R.
산업기밀 생성	산업활동 성과물 권리와 또는 영업비밀 관리	6.5000	.61835	10.89
	국가핵심기술의 관리	6.4444	.51131	10.42
	생성단계 관련자 최초 보안교육 실시	6.2222	.73208	8.89
	직무발명 보상	5.7222	.89479	6.25
	기술계약 체결시 관리	6.1111	.83235	8.53
	국가핵심기술의 수출시 관리	6.0556	.80237	8.28
	전략기술 · 전략물자의 수출시 관리	5.8333	.51450	6.72
	산업기밀관리 외부 위탁	5.8889	.58298	6.92
산업기밀 활용	제3자 제공시 관리	6.1111	.47140	8.33
	제공받은 산업기밀의 보호	6.1111	.58298	8.39
	이전 또는 이전받는 산업기밀의 보호	5.8333	.51450	6.56
	산업기밀 해외 이전시 보호	6.1667	.78591	8.83
산업기밀 파기	파기규정 수립	5.8333	.78591	6.86
	파기시점	5.8333	.85749	6.94
	파기방법	5.8889	.83235	7.19

어 상대적으로 낮게 평가되었다. 이는 산업기밀 생성단계에서 공개나 비공개로 관리할 시 법적 보호요건이 달라지므로 전략적 선택이 중요하다는 패널들의 인식을 반영하고 있다 하겠다. 한편, 경제성이 있는 지식재산을 창출한 노고에 대한 정당한 보상은 우선 순위가 다소 밀리는 것으로 나타났다.

4.2 산업보안 관리과정 모델 제안

그러면 지금까지 논의된 사항을 종합하여 Fig. 5와 같은 산업보안활동 관리과정 모델을 제시한다. 이는 3개의 링(ring)이 순환하는 형태이며 하단 링은 산업기밀의 생성, 활용, 폐기에 이르는 '산업기밀 생명주기'를 나타내며 산업보안 관리과정을 보호대상의 라이프 사이클에 동기화 시켜야 함을 의미한다. 상단 외곽 링은 산업기밀 생명주기에 맞춰 산업보안 정책 구축(Building), 정책 운영(Operating), 운영 검토 및 개선(Reviewing and Improvement)의 3단계 순환 주기를 형성한다. 1단계인 산업보안정책 구축(Building)은 조직 내 산업보안정책을 수립하는 것으로서 관련 법령의 규제요건을 고려하여 산업보안 담당조직 구성 및 책임 설정, 산업기밀 식별, 산업기밀침해 위험관리, 예산, 침해사고 대응절차 등을 조직의 전략적 경영목표의 관점에서 규정한다. 2단계인 정책 운영(Operating)은 1단계의 실제 구현으로서 침해위험관리계획에 따라 우선순위에 의해 보호대책을 실행하며, 산업보안문화 형성과 보안직무 스킬 향상을 위한 교육 · 훈련 프로그램을 실시한다. 3단계인 운영 검토 및 개선(Reviewing and Improvement)은 내외부의 산업보안 여건 변화, 산업기밀침해 잔류 위험수준, 관리체계 운영 효율성 등을 파악하고 주기적인 보안감사를 시행하여 1단계로 발전적 환류를 시키는 것이다. 비교 대상 ISMS들과 달리 제안 모델에서는 검토(Check)와 개선(Act)단계를 통합하여 관리주기가 기존 4, 5단계에서 3단계로 줄었는데 이는 즉시 개선이 가능한 것과 차후 정책 재수립에 반영할 사항을 분리하여 검토 결과를 신속히 현장

Fig. 5. Industrial security management circular model

반영하고 프로세스 단순화로 단계별 문서화 등에 대한 내부적 역량 소모를 줄여 산업보안관리체계의 전반적인 효율성을 높이기 위함이다. 박승욱 외(2010)도 국가 표준 R&D 프로세스를 PDCA사이클 기준으로 재구성하면서 검증(Check) 및 개선(Act) 단계를 통합하여 표현하고 있다. 상단 내부 링은 산업보안정책 구축에 부속되는 '산업기밀침해 위험관리 프로세스'로서 국내 ISMS들의 관리과정에서는 이를 별도의 단계로 운영하고 있으나 본 모델에서는 ISO/IEC 27001의 그것과 마찬가지로 산업보안정책 수립단계에 배치하여 전체적인 연계성을 높이고 수립단계에서부터 산업기밀침해 예방관리기능을 보다 강화하였다.

5. 결 론

본 연구에서는 '산업보안활동 관리과정 모델'을 2차에 걸친 델파이 조사와 통계분석으로 그 타당성을 검증하였다. 모델은 산업기밀 생명주기에 맞춰 산업보안정책 구축(Building), 정책 운영(Operating), 운영 검토 및 개선(Reviewing and Impro-

vement) 등 3단계 11개 통제항목들로 구성되는 ‘BORaI 순환주기’와 산업기밀의 생성, 활용, 폐기과정에 따른 15개의 통제항목들로 이루어진 ‘산업기밀 생명주기’를 그 구성요소로 하고 있다.

기술적 통제처리 결과 2개 사이클 구성 통제항목에 대한 타당성과 전문가 패널 의견합의정도가 높음을 보여주었고, 보다 정밀한 의견일치도를 측정하기 위한 켄달의 W검증 결과도 이에 부합함을 확인할 수 있었다. ‘BORaI 순환주기’는 연구모델의 메인 사이클로서 체계 개선 운영 모델인 PDCA 모형처럼 단계별 순차 이행으로 1단계로의 선순환적인 환류가 지속되는 것이다. ‘산업기밀침해 위험관리 프로세스’는 델파이 조사결과에서 보이는 것처럼 기존의 K-ISMS나 PIMS와 달리 ‘BORaI 순환주기’ 1단계인 ‘산업보안정책 구축’내에 편입하여 보안정책과의 연계성을 높였다. 따라서 연구모델은 단축된 3단계 순환주기를 통해 산업보안관리체계 개선활동의 신속성을 높이고, 산업기밀침해 위험관리를 주(主) 사이클의 1단계에서부터 가동하여 체계 운영의 효율성 향상을 추구하였으며, 산업기밀 생명주기를 모델 기저에 표현하여 주 사이클과 보호객체와의 동기화(同期化)를 명확히 하였다는 점에서 기존 ISMS들의 그것과 차별화 되었다고 본다. 제안된 모델은 조직의 산업보안정책 수립에 활용하여 비재무적 리스크로 인한 재난을 사전에 방지하는데 기여할 수 있을 것이다. 한편, 산업보안관리의 순환적 개선체계 프레임으로서는 의의가 있으나 각 단계를 조직 또는 운영수준의 산업보안 관리항목까지는 구체화하지 못하였다. 이에 대한 보안통제 프레임과 그 적용사례 등이 추가적으로 연구되어야 할 것이다.

References

Choi, H.K. (2009) *Comparative Study on social welfare facilities evaluation system of Korea and Japan*, Ph.D. dissertation, Dankook university, Seoul, Korea.
 FSA (2009) *Finance sector IT compliance analysis report*, FSA, Seoul, Korea.
 FSA (2011a) *Finance IT security compliance research report*, FSA, Seoul, Korea.
 FSA (2011b) *Introduction to ISMS and PIMS framework*, FSA, Seoul, Korea.

ISO/IEC (2005a) *ISO/IEC 27001, Information technology - Security techniques - Information security management systems - Requirements*, ISO/IEC, Geneva, Switzerland.
 ISO/IEC (2005b) *ISO/IEC 27002, Information technology - Security techniques - Information security management systems - Code of practice for information security management*, ISO/IEC, Geneva, Switzerland.
 Jang, J.K., Lee, S.H. and Choi, J.Y. (2011) Study on risk management process improvement for CMMI based IT project, *Journal of KIPS autumn conference*, Vol. 18, No. 1, pp. 1356-1359.
 Jeong, C.W., Lee, J.T., and Jeong, D.K. (2011) A Study on the Security Management System Model for the Information Security of the Aviation infrastructure, *Journal of CALSEC*, Vol. 16, No. 4, pp. 87-96.
 KCC (2010) *Notification on ISMS certification and etc. No. 2010-3*, KCC, Seoul, Korea.
 KCC (2011) *KCS.KO-12.0001, Personal Information Management (PIMS)*, KCC, Seoul, Korea.
 KISA (2007) *Study on personal information protection index model development and practical use*, KISA, Seoul, Korea.
 KRIHS (2009) *Easy to understand Homeland research methodology*, KRIHS, Anyang, Korea.
 MOTIE (2010) *Detailed security control implementation guideline for SME's technology protection*, MOTIE, Seoul, Korea.
 Oh, H.R., Oh, S.S., Kim, S. and Yeom, H.Y. (2005) Information standardization item definition and roadmap, *Review of KIISC*, Vol. 15, No. 5, pp. 67-82.
 Park, I.B. and Kim, J.D. (2011) Study on policy management Critical Success Factor for Industrial security culture formation, *Journal of Korean Association for Industry Security*, Vol. 2, No. 1, pp. 33-46.
 Park, S.W., Hong, J.W., and Kim, M.W. (2010) Analysis and proposal for planning phase strengthening of National R&D project, *Venture foundation research*, Vol. 5, No. 3, pp. 1-25.
 Shin, S.H., Yim, K.H., Kwon, O.J., Seo, H.S., Oh, J.I. and Kim, Y.C. (2007) An Empirical Study on the Effect of the BSC Application on the Organizational Performance in the Public Sector (focus on PDCA model), *Proceedings of KMIS autumn conference*, Seoul, Korea, pp. 102-108.
 TTA (2006) *TTAS.KO-12.0036, ISMS building guideline* TTA, Seong-Nam, Korea.

© Received January 22, 2013
 © Revised January 24, 2013
 © Accepted April 15, 2013