CxO가 알아야 할 정보보안

강은성 지음

한빛미디어 Hanbit Media, Inc.

CxO가 알아야 할 정보보안

강은성 지음

한빛미디어 Hanbit Media, Inc.

CxO가 알아야 할 **정보보안**

초판발행 2015년 2월 26일

지은이 강은성
펴낸곳 한빛미디어(주) / **주소** 서울시 마포구 양화로 7길 83 한빛미디어(주) IT출판부
전화 02-325-5544 / **팩스** 02-336-7124
등록 1999년 6월 24일 제10-1779호
ISBN 978-89-6848-751-4 15000 / **정가** 15,800원

총괄 배용석 / **책임편집** 김창수 / **기획·편집** 정지연
디자인 표지/내지 여동일, 조판 최송실
마케팅 박상용 / **영업** 김형진, 김진불, 조유미

이 책에 대한 의견이나 오탈자 및 잘못된 내용에 대한 수정 정보는 한빛미디어(주)의 홈페이지나 아래 이메일로 알려주십시오.
한빛미디어 홈페이지 www.hanbit.co.kr / **이메일** ask@hanbit.co.kr

Published by HANBIT Media, Inc. Printed in Korea

지금 하지 않으면 할 수 없는 일이 있습니다.
책으로 펴내고 싶은 아이디어나 원고를 메일(ebookwriter@hanbit.co.kr)로 보내주세요.
한빛미디어(주)는 여러분의 소중한 경험과 지식을 기다리고 있습니다.

저자 서문

2014년은 대한민국 정보보호의 역사에서 한 획을 긋는 해가 될 것 같다. 새해 벽두부터 터진 일련의 대규모 개인정보 유출 사건으로 사회와 기업에서 정보보호를 보는 눈이 크게 달라졌다. 클라우드, 빅데이터, 사물인터넷 등 미래의 정보기술을 논의할 때에도 정보보호는 중요하게 다뤄진다. 이제 우리 사회의 정보보호 수준을 높이지 않으면 겉으로 화려해 보이는 단말과 서비스, 인프라들이 사상누각이 될 수도 있다는 우려를 많은 국민이 하게 된 것 같다.

정보보호전문업체에서 연구소장과 보안대응센터장으로서 글로벌 보안 공격에 대응하며 정보보호제 품을 연구·개발했고, 무수한 공격이 들어오는 대형 포털 회사에서 최고보안책임자(CSO) 겸 개인정보호책임자(CPO)로 수년간 일한 나 역시 그러한 생각에 완전히 동의한다. 나는 기업의 정보보호 수준을 높이는 것이 사회의 정보보호 수준을 높이는 데 관건이라고 생각한다. 따라서 정부와 국회의 입장이 아니라 기업의 입장에서, 정보보호 솔루션의 공급자 입장이 아니라 수요자 입장에서, 그리고 이용자와 시민의 입장이 아니라 정보보호책임자의 입장에서 정보보안을 다루는 것이 매우 중요하다. 기업이 개인정보보호와 정보보호의 책임을 다하지 못했다는 비난을 받고 있지만, 그렇기에 더욱 사업자와 수요자, 정보보호책임자의 마음으로 생각하고 지원하고 실행하는 것이 필요하다.

정보보호책임자는 기업에서 정보보호최고책임자(CISO), 최고보안책임자(CSO), 개인정보보호(관리)책임자(CPO), 신용정보관리·보호인, 정보보안팀장, 개인정보보호팀장 등의 직책을 갖고 있다. 이들은 회사와 사업의 보안 위험을 최소화하기 위해

정보보호 거버넌스 구축, 관리 체계 수립과 중요 자산 보호, 위기관리, 규제 대응의 과제를 감당해야 한다. 그러기 위해서는 무엇보다 보안 임원뿐 아니라 CEO를 비롯한 CFO, CIO 등 회사 주요 임원이 스스로 기업 보안의 주체임을 인식하고 적극적으로 대응해야 한다. 기업의 주요 위험인 법규, 재무, 평판, 재난, 기밀·개인정보 위험의 대부분이 기업의 보안 위험에 포함되기 때문이다. 이것이 이 책의 제목을 'CxO가 알아야 할 정보보안'이라고 붙인 이유다.

이 책의 1장에서는 법과 표준, 기업 사례를 바탕으로 정보보호책임자의 임무와 업무를 기술하였다. 2장은 요즘 기업 보안의 근간으로 떠오르고 있는 정보보호 거버넌스를 실제 기업의 관점에서 다뤘다. 이제 정보보호는 정보보호책임자 혼자 힘으로 감당할 수 있는 문제가 아니라 이사회와 CEO, C 레벨 임원 등 회사의 최고경영진들이 다뤄야 할 회사 차원의 위험이기 때문에 회사의 경영, 조직, 투자, 문화 등 회사의 정보보호 거버넌스 업무를 구체적으로 살펴봤다. 3장은 관리 체계와 중요 자산 보호 업무에 관한 내용이다. 보안 위험 관리, 정보보호 대책의 수립과 이행, 협업 관리, 인력관리 등 대다수 정보보호책임자들이 가장 많은 시간을 들이는 업무의 핵심적인 관리 포인트를 짚고자 했다. 4장은 위기관리에 관한 장이다. 기존 정보보호 분야에서는 사고 대응 정도로 다루어 온 주제인데, 나는 이걸 기업의 위기관리 측면에서 다뤄야 한다고 보기 때문에 위기관리를 위기 전 업무와 위기 후 업무로 나누고 구체적인 예를 들어 상세하게 기술하였다. 5장에서는 규제 대응을 다뤘다. 법적 규제가 크게 강화되면서 기업 입장에서 이에 대응하기 위한 구체적인 방법에 관심을 갖다 보니 법 전공자도 아니면서 법에 대한 이야기를 길게 쓰게 되었다. 정보보호책임자가 중점적으로 보고 대처해야 할 내용을 중심으로 기술하였다. 6장은 정보보호

책임자의 역량과 업무 처리에 관한 장이다. 다들 본인이 중요하게 여기는 역량과 업무처리 기술이 있을 것이다. 이 장에서도 필요한 '생활의 지혜'를 얻어 가길 바란다.

여기에 쓰여진 내용은 나의 경험과 연구가 1차적인 바탕이 되었지만, 정보보안 분야 주요 리더의 집단 지성의 소산이기도 하다. 책을 기획하면서 어떤 내용이 들어가면 좋을지 조언을 듣기도 했고, 책을 쓴 뒤에는 내용에 대한 의견도 청취하여 보완하였다. 이 자리를 빌어 네이버 이준호 이사, 롯데카드 최동근 부문장, 넥슨 신용석 글로벌보안본부장, 네오위즈게임즈 최중섭 CISO, 이베이코리아 길기현 상무 등 정보보호책임자와 연세대 정보대학원 김범수 교수, 정보보호전문업체 (주)소만사의 김대환 대표이사 등 도움을 주신 모든 분께 깊이 감사 드린다. 특히 이 책의 법 관련 부분을 감수해 주신 강태욱 변호사(법무법인 태평양)께도 이 자리를 빌어 깊은 감사의 말씀을 드린다.

집과 도서관, 많은 사람과의 만남의 장소를 오가며 책을 쓰는 동안 25년이 훌쩍 넘는 직장 생활 중 처음으로 가족과 오랫동안 가까이할 수 있었던 것은 내게는 매우 특별한 경험이었다. 늘 함께 하는 가족이 고맙다.

부족한 점이 많지만, 이 책이 좋지 않은 여건에서 기업의 정보보호 업무를 수행하는 모든 정보보호책임자와 기업의 보안실무자, 정보보안 분야에 관심을 가지고 준비하는 청년, 청소년, 그리고 무엇보다도 기업 경영에 고민이 많을 CEO를 비롯한 CxO 여러분께 조금이나마 도움이 된다면 내게는 더할 나위 없는 기쁨이 되겠다.

개포도서관에서

강은성

저자 소개

저자_ **강은성**(CISO Lab 대표)

소프트웨어 개발자로 시작하여 국내 최대 보안 전문업체에서 연구소장과 시큐리티 대응센터장을 거쳐 굴지의 인터넷 포털회사에서 최고보안책임자(CSO)를 역임한 국내 최고의 보안전문가다.

그는 대기업 임원으로서 기업 보안을 책임졌던 리더십과 보안 현업에서 얻은 풍부한 관리·기술적 경험을 토대로 한국정보보호학회, 한국CPO포럼, 한국CSO협회 등 정보보호 관련 학회와 협회에서 활동하며 이론적 기반도 탄탄히 해왔다. 또한, 삼성전자 소프트웨어센터와 안철수연구소에서 보안 기술 및 제품을 연구·개발한 기술 역량, SK커뮤니케이션즈에서의 위기관리 경험을 바탕으로 실효성 있는 기업 보안 거버넌스와 정보보호 대책, 보안 위기관리 방안을 제안하고 있다.

지금은 CISO Lab을 설립하여 보안 위협의 변화뿐 아니라 기업의 조직 변화, 법·규제 같은 기업 환경의 변화에 대응하여 CEO, 정보보호최고책임자(CISO), 개인정보보호책임자(CPO) 등이 해야 할 기업 차원의 보안 위험 대응 전략을 탐구하여 기업 보안 컨설팅과 보안 교육을 진행하고 있다. 현재 〈아이뉴스24〉와 〈CIO〉에 보안 칼럼 「강은성의 CISO 스토리」, 「강은성의 Security Architect」를 연재하며, 저서로는 『IT시큐리티』(한울, 2009)가 있다.

감수자 소개

감수자_ 강태욱

개인정보보호 및 지식재산권 분야의 전문 변호사다. 2002년 판사로 임관한 이래 2007년까지 판사로 근무하다가 이후 법무법인(유한) 태평양에서 현재까지 구성원 변호사로 일하고 있다. 법원에서 지적재산권 전담부에서 근무한 경험을 바탕으로 개인정보보호 관련 민·형사 소송 및 자문, 지식재산권 관련 민·형사 소송 및 자문, 전자상거래와 게임 등 인터넷 기업 관련 법률 자문 및 소송 업무를 담당하고 있다.

또한, 행정자치부 개인정보보호 법령해석 심의위원, 국가지식재산위원회 전문위원, 게임콘텐츠등급분류위원회 위원, 한국저작권위원회 찾아가는 저작권 종합서비스 지원단 전문위원 등으로 활발한 사회 활동을 하고 있으며, 개인정보보호 업무에 기여한 공로를 인정받아 2013년에 안전행정부 장관 표창을 받은 바 있다.

추천사

정보보호와 관련된 많은 서적이 출간되었으나 실무 경험을 바탕으로 실질적 도움을 줄 수 있는 책이 늘 아쉬웠다. 이 책은 SK커뮤니케이션즈의 정보유출 사건을 대응하는 과정에서의 겪은 경험을 비롯하여 수십 년간 보안 현장에서 얻어진 생생한 지식과 대응책들이 녹아 있는 보물창고라고 생각한다. 특히, 금융, 공공 등 각 분야에서의 정보 문화와 거버넌스, 보안 및 인력 관리 체계와 규제 대응에 관한 내용은 보안 담당자와 책임자가 일상적으로 겪는 문제에 대해 생생한 해결책을 제시할 것이다. 이 책을 정보보호를 위해 고민하는 이들, 특히 기업 정보보호의 최종책임자인 경영진과 정보보호책임자에게 망설임 없이 추천할 수 있어서 기쁘다.

정태명(한국CPO포럼 회장, OECD 정보보호분과 부의장, 성균관대 소프트웨어학과 교수)

2013년 7월, 금융전산 보안강화 종합대책에서 발표된 CIO 겸직금지에 따라 은행권 최초로 전임 CISO에 임명되어, 지도에 없는 길을 가야 한다는 개척자의 마음으로 시작했던 기억이 납니다. 이 책에 담긴 법과 표준에 나타난 CISO 역할과 저자가 CISO로서 경험한 타 부서와 협업에 대한 중요성은 다른 책에서는 볼 수 없던 부분입니다. 이 책이 보안이라는 무거운 책임을 진 보안담당자들에게 든든한 반려자가 될 것이라고 믿습니다.

김종현(KB국민은행 정보보호본부장, 상무)

The hindsight is always 20/20(뒤돌아보면 모든 것이 명확하다).

2000년대 말부터 해마다 발생하고 있는 대형 개인정보 유출 사고 때문에 최근에는 기업마다 CISO라는 별도의 보안 임원을 두며, 보안에 대한 최고경영진의 투자도 활발한 편이다. 하지만 불과 수년 전만 해도 CISO라는 별도의 직책이 있는 기업을 찾기 어려웠던 것이 현실이다. 그런데 이 책의 저자인 강은성 대표는 소프트웨어 개발자로 시작하여 보안 전문업체에서 보안대응센터장과 연구소장을 거쳐 국내 굴지의 인터넷 기업에서 최고보안책임자(CISO)를 역임한 1세대 전문 CISO이다. 현재는 CISO Lab을 설립하여 정보보호 컨설팅과 교육 등을 통해 한국 사회 전반의 보안 수준을 높이기 위해 동분서주하고 있다. 본인도 최고 보안책임자로서 빅데이터, 사물인터넷, 간편 결제 활성화 등으로 새로운 보안 이슈가 등장할 때마다 강은성 대표에게 아이디어를 구하곤 한다.

강은성 대표가 이 책의 초안을 건넸을 때 본인도 이를 읽으며 그동안 현장에서 느꼈던 많은 부분이 일목요연하게 정리되었다. 특히 제4장(연습은 실전처럼, 실전은 없는 게 좋다)의 내용은 "The hindsight is always 20/20(뒤돌아보면 모든 것이 명확하다)"는 격언을 생각나게 하는 생생한 현장의 가르침이라 여러 번 곱씹으며 읽었다. 현재 CISO로 근무하는 보안인, CISO를 꿈꾸는 보안인, 보안의 중요성을 알고 싶은 최고경영진에게 이 책은 '탁상공론'이 아니라 발바닥에 불이 나도록 뛰어다녔던 전임 CISO가 들려주는 살아있는 현장의 가르침이 되리라 믿는다. 그리고 본인 또한 부디 이 책을 통하여 한국 기업의 보안 수준이 크게 향상되기를 기대해 본다.

이준호(이사, NAVER CISO)

강은성 대표는 실전경험이 풍부한 정보보호 전문가다. 정보보호전문업체에서 보안대응센터장과 연구소장으로서 글로벌 보안 공격에 대응하며 정보보호제품을 연구·개발했고, 무수한 공격이 들어오는 대형 포털 회사에서 최고보안책임자(CSO) 겸 개인정보관리책임자(CPO)로 수년간 일하였고, 그만큼 다양한 실무 경험을 갖춘 정보보호 전문가를 찾아보기 힘들다. 강 대표와 한국CPO포럼에서 오랫동안 같이 활동하면서 정보보호의 현실을 토론할 때마다 그가 보여준 깊이 있는 통찰력을 자주 보아온 나로서는 이 책의 가치가 얼마나 큰지 잘 알고 있다. 일련의 대형 정보유출사태가 불러온 강한 법규제는 정보보호를 법적 책임의 영역으로 끌어들였다. 기업이 정보보호를 잘하도록 그가 던지는 메시지는 핵심적이다. 기업 내부의 정보보호 거버넌스, 정보 자산 관리 체계, 위기관리 체계에 걸쳐 알토란 같은 노하우가 흘러넘친다. 법규제에 대해 심도 있고 체계 있게 정리하여 일목요연하게 알 수 있도록 정리한 것도 이 책의 장점이다. 이 책은 IOT 시대에 기업을 운영하는 CEO의 필독서다.

구태언(테크앤로법률사무소 대표변호사)

직장인으로서 정보보호임원(CISO)을 꿈꾼다면 필독을 권한다. CISO는 평상시에 대표이사와 마케팅, CRM, 재무, CIO 부서 등 회사의 주요 이해당사자와 어떻게 커뮤니케이션을 하고 이들을 설득해야 하는가, 개인정보 유출 사고 발생 시 검찰, 경찰, KISA, 금감원, 방통위, 미래부, 행자부, 변호사, 자문교수, 언론 등과 어떻게 커뮤니케이션을 해야 하는가 하는 질문에 대한 답을 얻을 수 있는, 현재까지 내가 알고 있는 바로는 유일한 책이다. 대기업 CISO로서 5년 동안의 경험을 바탕으로 솔직하고, 가감 없는 내용을 담고 있어서, 강은성 대표 본인만의 핵심 노하우가 너무 공개하는 것은 아닌지 살짝 우려되기도 한다. 이 책이 널리 퍼져서 우리나라 보안 생태계의 수준이 한 단계 더 높아지기를 바란다.

김대환 ((주)소만사 대표이사, 고려대학교 기술경영전문대학원 겸임교수)

차례

1

즐기는 자가 이긴다!

정보보호책임자

정보보호의 목적

개인정보보호와 정보보호

정보보호최고책임자

개인정보보호책임자

정보보호책임자의 업무

매일 아침 습관처럼 검색 사이트에서 '개인정보유출'이라는 단어를 검색하곤 한다. 하루도 관련 기사가 나오지 않는 날이 없을 정도다. 사건 자체가 최근에 발생한 것도 있지만, 많은 사건은 과거에 난 것이 요즘 밝혀진 것들이다. 수사 당국에서 강력한 수사를 천명하고 수사한 성과인 것 같다.

기업에서 최고보안책임자CSO, Chief Security Officer 겸 개인정보보호책임자CPO, Chief Privacy Officer로 일했던 나로서는 이런 기사들을 읽을 때마다 마음이 편하지 않다. 나도 한 사람의 시민이자 고객으로서 주장할 바가 있지만, 기업에서 개인정보를 비롯한 중요 자산을 보호하는 일을 해 왔고, 현재 시소랩CISOLab이라는 구멍가게를 열고 하는 사업 역시 기업이 당면한 정보보호 위험을 평가하고 보안 대책을 세워 정보보호 위기를 대비하는 일이기 때문이다. 그런 기사를 읽게 되면 분노하기보다는 자료를 찾아 원인을 분석함으로써 기업이 보안 사고를 예방하고 위기 발생 시 올바르게 대응함으로써 피해를 최소화하는 방안을 연구한다.

이러한 문제의식에서 1장에서는 이후 이 책의 내용을 관통하는 핵심적인 틀을 정립하고자 한다. 기업 밖에서 들려 오는 많은 주장과 논리가 있지만, 기업 관점에서, 그리고 정보보호최고책임자CISO, Chief Information Security Officer나 개인정보보호책임자 등 기업의 정보보호책임자 관점에서 이것을 재해석하고 대처 방향과 전략을 잡아 나가는 게 중요하리라 생각된다.

정보보호의 목적

기업에서 정보보호를 왜 하는가? 상투적인 질문이지만 한 번쯤은 짚고 넘어가

야 할 질문이다. 정보보호책임자 자신이나 산하 구성원들에게도 명쾌한 논리가 필요하며 회사 내 다른 부서의 임원, 직책자, 구성원들과 커뮤니케이션할 때 쓸 수도 있다.

정보보호 분야에서는 전통적으로 이 질문에 세 가지 답변을 해 왔다.

첫째, 사업을 보호하기 위해서다.

보안을 소홀히 해서 고객정보가 대량 유출되거나 산업기밀, 영업 비밀이 경쟁자에게 유출되면 사업이 어려워질 수 있고, 그에 따라 회사가 큰 영향을 받을 수 있다. 2013년 미국의 2위 소매유통업체인 Target사에서 발생한 1억 1천만 건의 개인정보 유출 사건이나 2014년 1월 국내 카드사들의 대규모 개인정보 유출 사건을 기업에서는 심각하게 받아들이고 있다. 해킹으로 네트워크가 마비되거나 서비스가 중단되는 것 역시 인터넷 기반 사업에 중대한 위협이 될 수 있다. 사업을 지속하려면 이러한 내·외부의 보안 위험을 예방하고, 사고 발생 시 신속하고 정확한 대응으로 기업의 위기를 최소화해야 한다.

둘째, 사업을 시작하기 위해서다.

어떤 사업은 정보보호 없이는 시작할 수 없다. 예를 들어, 온라인 교육사업을 시작한다면 이제는 '정보통신망 이용 촉진 및 정보보호 등에 관한 법률(정보통신망법)'에서 규정한 개인정보취급방침을 갖추고, 서비스 개발 시 고객의 개인정보를 수집·이용·제공하는 데 대한 고객의 동의를 받아야 하며, 개인정보를 보호하기 위한 기술적·관리적 보호조치 또한 구축해야 한다. 이런 최소한의 조치 없이는 고객이 모이지도 않고, 문제 발생 시 과태료, 과징금과 같은 행정처분뿐 아니라 형사처벌을 받을 수도 있다. 즉, 사업을 시작하지 않는 것이 더 나은 상황이 될 수도 있다.

셋째, 고객 가치를 창출하기 위해서다.

보안 제품이 아니면서 보안 기능이 고객 가치를 창출하는 경우는 거의 없었다. 보안에 대한 고객의 욕구가 증가하면서 스마트폰에 지문 인식 등 개인 인증 기능이 추가되었고, 팬택사의 베가 스마트폰에 들어간 시크릿 기능은 일반 제품에서 보안 기능이 고객 가치를 창출하는 새로운 장을 열었다. 이제 개인정보 이슈가 큰 금융부문에서도 정보보호를 강조하는 흐름이 나타날 가능성이 보인다.

정보보호의 목적에 대한 이러한 전통적 답변은 회사의 사업적 관점에서 여전히 유효하고, 고위 임원이나 사업 책임을 진 부서장에게는 절실하게 느껴질 수 있다. 하지만 임직원에 따라서는 이를 실감하지 못하는 경우가 있다. 전통적인 답변의 의미를 포함하면서 임직원 개인에게 좀 더 직관적으로 느껴지는 답변이 없을까 고민해 오다가 다음과 같이 정리하였다.

첫째, 나와 동료의 '성과'를 지키기 위해서다.

보험 사업의 핵심은 개인 고객을 모집하는 일이다. 한 사람의 개인 고객이 모집되면 이 고객에게 다양한 상품을 판매할 수 있고, 이 고객을 통해 다른 고객이 추가로 유입될 수도 있다. 다른 말로 표현하면 보험 사업의 핵심은 고객의 개인정보를 수집하는 일이다. 은행, 증권, 카드, 캐피탈 등 금융회사의 사업은 모두 개인정보 확보가 핵심 경쟁력이다. 이외에도 이동통신사업, 학습지사업 등 개인정보 기반의 사업은 매우 많다. 이렇게 임직원이 확보한 개인정보를 도난당하면 사업 지속성에도 타격이 있지만, 무엇보다도 임직원의 노력이 헛되게 된다. 개인정보를 지키기 위해 보안을 강화하는 일은 바로 나와 동료, 부하 직원이 흘린 땀의 성과를 지키는 일이다.

둘째. 나와 동료의 위험을 줄이기 위해서다.[01]

회사 임직원이 고객의 주민등록번호를 자신의 PC에 암호화하지 않은 채로 저장한 것이 적발되면, 사업자가 개인정보보호법과 정보통신망법 위반으로 과태료를 부과받을 수 있다. 실제로 회사가 이런 과태료 처분을 받는다면 개인에게도 불이익이 돌아갈 것이다. 더욱이 전·현직 개인정보취급자가 퇴사하면서 자신의 PC를 통째로 백업받아서 그것을 가지고 나간다면 형사처벌을 받을 수 있는 개인정보 유출 사건이 될 수 있다. 이를 막기 위해서는 회사와 구성원이 개인 PC에 암호화하지 않은 개인정보를 갖고 있지 않도록 노력하고, 개인정보 탐지 및 암호화 솔루션을 회사의 모든 PC에 적용하는 것이 좋다. 회사에서 이 솔루션을 구매하여 제공하는 것은 회사를 위한 일이기도 하지만 동시에 내 위험을 줄이는 일이기도 하다. 이러한 상황은 내 동료에게도 발생할 수 있다. 이를 예방하기 위해 정보보호 조직이 하는 활동은 동료를 위한 활동이기도 한 것이다. 정보보호 인력들은 이러한 사명감과 자부심을 품고 업무를 하기 바란다.

그 밖에도 각자가 처한 환경과 개인 특성에 따라 다양한 정보보호의 목적이 있을 것이다. 그것이 무엇이든 나와 부서원이 하는 정보보호 활동이 회사의 사업과 동료, 부하 직원을 위한 것이라는 믿음이 있으면 좋겠다. 구성원의 불편을 일부 초래하기도 하지만 그래야 일이 재미있고, 어려운 일이 있어도 헤쳐나갈 수 있다. 또한, 이런 관점을 가지면 정보보호업무의 주체는 정보보호 조직만이 아닌 모든 구성원이 되고, 정보보호 활동은 각자가 자신을 위해 하는 활동이 된다.

---

01 **저자주_** 정보보호의 목적이 나와 동료의 성과를 지키기 위한 것이라는 첫째 설명은 사업 지속성을 위한 전통적인 설명과 일치한다. 정보보호 활동의 적극적인 측면, 또는 회사의 긍정적 측면의 지원이라고 부를 수 있다. 그에 반해 나와 동료의 자리를 지키는 둘째 목적은 정보보호 활동의 소극적 측면, 또는 회사의 부정적 측면의 보완이라고 설명할 수 있다.

개인정보보호와 정보보호

앞에서 눈치챘을지 모르겠다. 정보보호의 목적이라고 쓴 내용은 개인정보보호의 목적이라고 바꿔 불러도 별 무리가 없다. 정보보호의 목적을 설명하는 일부 내용에 그 예로 개인정보보호를 넣기도 했다.

전통적으로 정보보호Information Security에서 보호하려는 대상은 정보 자산Information Asset이다. 정보 자산에는 크게 정보(콘텐츠)와 그것을 처리하는 정보처리시스템이 포함된다. 대표적인 정보로는 금융정보, 신용정보, 산업기밀, 마케팅정보, 의료정보, 군사정보, 개인정보가 있다. 따라서 개인정보는 정보보호 대상의 하나인 셈이다.

하지만 개인정보는 기업에서 관리하는 다른 정보들과 차이가 있다. 개인정보는 사업자가 정보주체(고객)의 동의를 받아서 수집·이용하는, 정보주체에 관한, 정보주체 소유의 정보다. 특히, 고객 개인정보 기반의 사업이 많다 보니 사업자가 정보주체의 동의 없이 개인정보를 자신의 이익을 위해 활용하여 고객에게 피해를 줄 수 있다. 즉 산업기밀이나 마케팅정보 등 정보보호의 다른 대상과는 달리 개인정보는 사업자와 정보 소유자의 이해관계가 상충할 수 있다. 그래서 개인정보 관련 법규들은 수집·보관·이용·제공·파기의 개인정보 생명주기에서 사업자의 의무를 세부적으로 규정하고 있다. 예를 들어, 개인정보를 수집·이용하거나 제3자에게 제공할 때 반드시 정보주체의 동의를 받아야 하고, 동의받은 목적 안에서만 그것을 활용해야 하며, 정보주체가 자신의 개인정보의 열람·정정 등을 요구하거나 개인정보 사고 등이 발생했을 때 정보주체와 책임 있게 소통해야 한다. 개인정보 보호에 관한 사항을 일반법으로 집대성한 개인정보보호법

이나 정보통신서비스 제공자[02]에게 적용되는 정보통신망법의 개인정보보호 조항들, 신용정보법의 개인신용정보보호에 관한 조항들이 바로 그것이다. 이는 정보보호에서 다루는 다른 정보와 개인정보 사이의 가장 큰 차이점이다.

또한, 개인정보보호 관련 법규에서는 사업자가 수집하여 이용하는 개인정보를 안전하게 관리할 것을 규정하였다. 이 법들의 소관부처에 제정한 관련 고시에는 개인정보를 보호하기 위한 관리적·기술적·물리적 보호조치가 상세하게 기술되어 있다. 개인정보보호법의 '개인정보의 안전성 확보조치 기준(행정자치부의 고시)', 정보통신망법의 '개인정보의 기술적·관리적 보호조치 기준(방송통신위원회 고시)', 신용정보법의 '신용정보업 감독규정(금융위원회 고시)' 중 '기술적·물리적·관리적 보안 대책 마련 기준(제20조 별표3)'이 바로 그것이다. 이름도 매우 비슷한 이 세 고시는 개인(신용)정보를 보호하기 위해 접근 권한 관리, 비밀번호 관리, 접근통제 시스템 운영, 접속기록 보관 같은 대부분의 공통적인 내용과 물리적 보안, 영상정보처리기기 보안 등 법 적용 부문의 특성을 반영한 약간의 조항으로 이뤄져 있다. 전체적으로 이러한 개인정보 안전성 확보대책은 DB 보안, 서버 보안 등 IT 인프라 보안과 서비스 및 애플리케이션 보안, 콘텐츠 보안, 개발 보안 등 전통적으로 정보보호에서 다뤄온 주제와 별반 다르지 않다. 종합하면 개인정보보호와 정보보호는 중요 자산을 안전하게 보호하기 위한 많은 공통점과 개인정보 생명주기 동안 정보주체의 권리를 보호하기 위한 사업자의 의무라는 개인정보 특성에서 오는 일부 차이점이 있다.

---

02 **저자주_** 정보통신서비스 제공자는 "전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 영리적인 목적으로 정보를 제공하거나 정보의 제공을 매개하는 자"(정보통신망법 제2조 1항)인데, 한마디로 하면 통신사업자와 통신사업자의 망을 이용하여 서비스를 제공하는 영리사업자다. 인터넷을 이용하는 비영리 제공자인 정부나 시민단체 등은 여기에 포함되지 않는다. 이 책에서는 주로 제공자라는 가치 중립적인 표현보다는 사업자라고 해서 좀 더 영리적인 목적이 있음을 표현하고자 했다.

많은 기업에서 개인정보는 보호해야 할 여러 정보 중 가장 중요한 정보의 하나다. 은행, 보험사 등 금융회사뿐 아니라 건설사, 통신사, 게임사, 쇼핑몰, 여행사 등 개인 고객을 상대하는 모든 회사에서 고객의 개인정보는 사업의 바탕을 이룬다. 이는 개인정보의 종류나 양에서 약간의 차이가 있을 뿐이다. 이러한 기업에서 개인정보는 그 무엇보다도 보호해야 할 핵심 자산이다. 휴대폰이나 자동차 등 과거에는 물건만 팔면 되던 제조업체도 이제는 사후 서비스, 기술지원 등을 온라인으로 제공함으로써 고객과의 지속적인 커뮤니케이션을 시도한다. 제조업체에서도 산업기밀뿐 아니라 수집한 개인정보의 보호 역시 중요한 과제가 되었다.

B2B 사업자는 개인정보 수집의 필요성이 상대적으로 덜하다. 철강, 반도체, 조선 등 기업고객 대상의 사업자는 대부분 설계도와 같은 산업기밀의 보호가 정보보호의 핵심 과제로 여겨져 왔다. 하지만 개인정보보호법이 시행된 이후로 임직원과 협력업체, 대리점, 투자자 등 비고객의 개인정보 역시 개인정보 보호의 대상이 되어서 개인정보 보호도 소홀히 할 수 없는 업무가 되었다. B2C, B2B 사업자를 막론하고 대다수 기업에서 개인정보가 정보보호의 핵심 대상이 된 것이다.

기업의 정보보안팀이 참여하는 침해사고대응팀협의회(CONCERT)에는 약 320개의 회원사가 있다. 이는 우리나라에 적어도 320개 이상의 회사에 팀 또는 파트 수준의 정보보호 조직이 있다는 것을 뜻한다. 이 조직들이 기업 중요 자산의 관리적·기술적·물리적 보안을 담당하고 있다. 이는 개인정보보호와 정보보호의 공통 부분이다. 개인정보 생명주기에서 정보주체의 동의와 같이 개인정보보호에 특수한 부분은 개인정보 담당자가 담당하는 것이 보통이다. 별도의 개인정보 보호조직에 속한 인력은 많지 않지만 말이다.

업무 측면에서는 개인정보 담당자가 좀 더 법과 가까이 있으면서 법에 기반을 둔 개인정보보호 정책과 지침을 수립하여 전사적으로 추진하는 업무를 담당한다. 개인정보 담당자 중 법 전공자를 종종 만나게 되는 이유다. 이들은 서비스 기획부서나 법무부서, 고객대응부서와의 협업도 필수고, 개인정보 영향평가나 개인정보 수탁사 관리 업무도 담당한다. 정보보호 담당자들은 전사 정보보호 정책과 지침을 수립하고, 회사의 중요 자산을 보호하기 위한 관리적·기술적·물리적 보호 대책을 수립하며 협업 부서와 함께 구현한다. 개인정보 담당자보다 보안이나 IT 출신 인력이 많이 포진해 있다.

정보의 특성, 기업과 조직, 업무 등 여러 측면에서 볼 때 개인정보보호와 정보보호는 법적, 기업적, 조직적, 업무적 측면에서 통합적으로 이해하고 관리해야 한다고 여겨 이 책에서는 별도로 표시하지 않으면 정보보호업무에 개인정보보호업무가 포함되는 것으로 가정하였다. CPO도 법률뿐 아니라 기술적·관리적 보안 대책도 이해하길 바라고, CISO도 개인정보를 비롯한 정보보호 관련 법규에 익숙해지기를 바란다. 그래야 어떤 직무를 맡은 정보보호책임자든지 개인정보를 비롯한 기업의 중요 자산을 지킬 수 있다.

정보보호최고책임자

정보보호 분야에서 법이 미치는 영향이 갈수록 커지고 있다. 여섯 달도 안 되는 짧은 기간이었지만 처음 CSO를 맡았던 2008년만 해도 법적 이슈가 크지 않았다. 법에서 정한 정보보호 관련 내용을 들여다보기는 했지만 '밑줄 쫙쫙 치면서' 상세하게 읽을 필요는 느끼지 못했다. 그보다 정보보호업무를 잘 해내는 것이 훨씬 중요했다. 하지만 시대가 확실히 바뀌었다. CISO(정보보호최고책임자)의

중요한 역량 중의 하나가 정보보호 관련 법 규정을 정책과 기술 관점에서 풀어내는 것이 되었다. 이것이 CISO의 임무와 업무를 얘기하면서 법 얘기부터 꺼내는 이유다.

2013년 몇몇 은행과 언론사의 전산망 마비로 사회적 물의를 빚은 3·20 사태 이후 금융권의 CIO-CISO 분리가 사회적 관심사로 떠올랐다. 전자금융거래법에는 "금융회사 또는 전자금융업자는 전자금융업무 및 그 기반이 되는 정보기술 부문 보안을 총괄하여 책임질 정보보호최고책임자를 지정하여야 한다"(제21조의2 제1항)고 CISO 지정이 의무화되었지만, 3·20 사태 때까지 별도의 CISO를 임명한 금융회사는 거의 없었다. 법의 취지와는 달리 대부분 금융회사에서는 CIO(최고정보책임자)가 CISO를 겸임해 온 것이다. 3·20 사태 이후 금융권의 정보보호 이슈가 큰 사회적 문제로 대두하자 같은 해 7월 금융위원회는 '금융전산 보안 강화 종합대책'에서 CISO의 독립성 강화를 중요한 의제로 삼긴 했지만, CIO와 CISO 분리 대상의 요건을 자산 2조 원, 직원 수 300명에서 자산 10조 원, 직원 수 1500명으로 크게 높이면서 대상 금융회사가 36개에 불과해 실효성은 크지 않으리라고 예측됐다. 그러다가 작년 말부터 2014년 상반기 사이에 은행과 카드사에서 대규모 개인정보 유출 사건이 발생하면서 CIO와 CISO 분리가 다시 사회적 관심사가 되었고, 이를 반영하여 2014년 10월에 전자금융거래법 개정되었다.

CISO 조직을 CIO 조직으로부터 분리한다고 금융회사의 정보보호 문제가 일거에 해결되지는 않을 텐데 이것을 마치 금융권 정보보호 수준의 잣대인 것처럼 쓰는 기사들을 보면 우려할 만한 점이 있지만, 개인정보나 금융정보, 신용정보, 전자금융 시스템과 같이 국가 경제의 인프라이자 대다수 국민의 금융자산을 관리하는 일정 규모 이상의 금융회사라면 CEO에게 보고하는 독립된 임원

급 CISO의 존재는 필수불가결한 것 역시 사실이다.

CISO 지정을 명시한 또 다른 법은 정보통신망법이다. 이 법에서는 임원급 CISO의 지정을 기업의 선택에 맡겼지만, 정보통신서비스 기업 중 임원급 전임 CISO가 있는 기업이 있다. 이는 보안의 필요성을 기업 스스로 느꼈기 때문이다. 정보보호의 중요성이 날로 높아지면서 정보통신망법에서도 일정 규모 이상의 업체는 임원급의 CISO 지정을 의무화하는 것으로 개정되어 2014년 11월 29일부터 시행되었다.

국가안전보장·행정·국방·치안·금융·통신·운송·에너지 등의 업무와 관련된 시스템과 정보통신망 보호를 목적으로 하는 정보통신기반보호법에서도 국가의 "주요 정보통신기반시설의 보호에 관한 업무를 총괄하는 정보보호책임자를 지정하여야 한다"(제5조 제4항)고 하였다. 법이 이렇게 변화하는 추세라면 향후 CISO를 지정하는 기업이 상당히 늘어날 것으로 보인다.

법에 나타난 CISO의 업무 ——

지금부터 CISO의 업무를 좀 더 세부적으로 살펴보자. 정보통신망법에는 정보보호최고책임자가 다음 업무를 총괄한다고 되어 있다(제45조의3 제3항).

표 1-1 정보통신망법에 나타난 정보보호최고책임자의 총괄 업무

제45조의3 제3항	분류
1 정보보호관리 체계의 수립 및 관리·운영	정보보호 관리 체계의 수립·운영
2 정보보호 취약점 분석·평가 및 개선	보안 취약점 분석
3 침해사고의 예방 및 대응	정보보호 대책 수립·이행, 사고 대응
4 사전 정보보호 대책 마련 및 보안조치 설계·구현 등	정보보호 대책 수립·이행
5 정보보호 사전 보안성 검토	정보보호 대책 수립·이행

제45조의3 제3항	분류
6 중요 정보의 암호화 및 보안서버 적합성 검토	정보보호 대책 수립·이행
7 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행	규제 대응

이 법 조항을 분류하면 CISO는 ▲정보보호 관리 체계의 수립·운영(1) ▲보안 취약점 분석과 정보보호 대책 수립·이행(2, 3, 4, 5, 6), ▲사고 대응(3)의 업무를 총괄한다고 할 수 있다.

전자금융거래법과 그 시행령을 종합하면 정보보호최고책임자는 다음과 같은 업무를 수행한다(제21조의2 제3항, 시행령 제11조의3 제2항).

표 1-2 전자금융거래법과 그 시행령에 나타난 정보보호최고책임자의 업무[03]

제21조의2 제4항[03]과 시행령 제11조의3 제2항	분류
1 전자금융거래의 안정성 확보 및 이용자 보호를 위한 전략 및 계획의 수립	정보보호 거버넌스 수립·운영
2 정보기술 부문의 보호 및 관리	정보보호 대책 수립·이행
3 정보기술 부문의 보안에 필요한 인력관리 및 예산편성	정보보호 관리 체계의 수립·운영
4 전자금융거래의 사고 예방 및 조치	정보보호 대책 수립·이행, 사고 대응
5 전자금융업무 및 그 기반이 되는 정보기술 부문 보안을 위한 자체심의에 관한 사항	정보보호 대책 수립·이행
6 정보기술 부문 보안에 관한 임직원 교육에 관한 사항	정보보호 관리 체계의 수립·운영

크게 보면 전자금융거래와 정보기술 부문을 포함하여 ▲정보보호 거버넌스 수립(1) ▲정보보호 관리 체계의 수립·운영(3, 6) ▲정보보호 대책의 수립·이행(2, 4, 5) ▲사고 대응(4)을 주요 업무로 분류할 수 있다. 전자금융거래 부문에 관한

03 **저자주_** 기존 전자금융거래법 제21조의2 제3항에 있던 조항이 2014년 10월 15일에 개정되면서 같은 조 제4항으로 옮겨졌다. 시행일은 2015년 4월 16일이다.

사항은 금융위원회 고시인 전자금융감독규정 제3장 '전자금융거래의 안전성 확보 및 이용자 보호'와 연결된다. 정보보호 조직의 장으로서 CISO의 업무에 관해서는 금융위원회와 금융감독원이 펴낸 『금융회사 정보기술(IT)부문 보호업무 이행지침』(2014)도 참고할 만하다.[04]

정보통신기반보호법과 그 시행령을 종합하면 정보보호책임자의 업무는 다음과 같다(제5조 제5항, 시행령 제9조 제2항).

표 1-3 정보통신기반보호법과 그 시행령에 나타난 정보보호책임자의 업무

제5조 제5항과 시행령 제9조 제2항	분류
1 주요 정보통신기반시설을 안전하게 보호하기 위한 물리적·기술적 대책을 포함한 관리대책의 수립·시행	정보보호 대책 수립·이행
2 주요 정보통신기반시설보호대책의 수립, 침해사고 예방 및 복구에 필요한 기술적 지원의 요청	정보보호 대책 수립·이행, 사고 대응
3 주요 정보통신기반시설의 취약점 분석·평가 및 이를 수행하는 전담반 구성	보안 취약점 분석
4 주요 정보통신기반시설의 보호에 필요한 조치 명령 또는 권고의 이행	규제 대응

04 **저자주_** 금융회사 정보기술(IT)부문 보호업무 이행지침(2014) 별첨1 '정보기술부문의 주요 업무 예시' 중 '4. IT 정보보호'에 다음 13가지를 꼽고 있다. 정보보호 조직 업무 작성 시 참고할 만하여 여기에 옮긴다.

- 취약점 분석·평가 및 그 이행 계획 수립 및 시행
- 내부 정보보호 정책 수립 및 정보보호 관련 규정·지침 제·개정
- 정보보호 아키텍처 유지 관리
- 정보보호 교육 계획 수립 및 교육 실시
- 전자금융 및 정보기술 부문 관련 보안성 검토
- 전자금융 관련 정보보호 대책 수립 및 시행
- 모의해킹, 디도스 대응 훈련 등 비상 대응훈련 계획 수립 및 실시
- IT 내부 통제(법규준수 포함) 관리
- 침해 시도에 대한 실시간 보안관제 및 통합보안관제시스템 운영
- 외부 직원 출입 통제 및 노트북, USB 등 반출·입 통제
- 침해 방지·대응 시스템 구축·운영
- 시스템 접근 통제, 권한 관리 및 사용자 인증 관련 시스템 구축·운영
- 고객 정보 보호 및 정보 유출 방지 시스템 구축·운영 등

제5조 제5항과 시행령 제9조 제2항	분류
5 주요 정보통신기반시설이 교란·마비 또는 파괴된 사실을 인지한 때에 관계 기관에 그 사실을 통지	사고 대응
6 침해사고가 발생한 주요 정보통신기반시설의 복구 및 보호에 필요한 조치	사고 대응
7 기타 다른 법령에 규정된 주요 정보통신기반시설의 보호업무에 관한 사항	규제 대응

정보통신기반보호법에서는 정보보호책임자의 업무를 ▲보안 취약점 분석 및 정보보호 대책의 수립·이행(1, 2, 3) ▲규제 대응(4, 7) ▲사고 대응(2, 5, 6)으로 보고 있음을 알 수 있다.

이상 CISO 지정과 업무를 규정하는 세 가지 법을 종합하여 재분류하면 다음 표와 같다. 표의 각 칸은 〈표 1-1〉, 〈표 1-2〉, 〈표 1-3〉에서 해당 분류에 포함된 항목 번호다. 한 항목이 여러 분류에 포함될 수 있게 하였다

표 1-4 관련 법에 나타난 CISO의 주요 업무 분류

분류 \ 법	정보통신망법	전자금융거래법	정보통신기반보호법	항목 수
정보보호 거버넌스	N/A	1	N/A	1
정보보호 관리 체계 수립·운영	1	3	N/A	2
보안 취약점 분석 및 정보보호 대책 수립·이행	2, 3, 4, 5, 6	2, 4, 5	1, 2, 3	11
규제 대응	7	N/A	4, 7	3
정보보호 위기관리	3	4	2, 5, 6	5

이 세 법을 살펴보면 CISO의 업무는 크게 ▲정보보호 관리 체계의 수립·운영 ▲보안 위험 분석과 정보보호 대책의 수립·이행·점검 ▲규제 대응 ▲정보보호 위기관리로 분류할 수 있다. 업무에 포함된 항목 수를 보면 CISO의 업무는 보안 취약점 및 정보보호 대책에 관한 것이 많음을 알 수 있다. 여기에서 '정보보

호 위기관리'는 사고 대응을 좀 더 확장한 분류다. 침해사고에 잘못 대응하면 회사의 위기까지 번질 수 있으므로 사고 대응을 관계기관에서 신고하고 필요한 복구를 하는 것과 같은 좁은 의미에 국한하지 않고, 위기관리로 좀 더 포괄적으로 해석하여 CISO의 업무로 정의하였다. 침해사고와 정보보호 위기의 관계, 그에 대한 대응에 관해서는 제5장에서 상세하게 다룬다.

표준에 나타난 CISO의 업무 ——

CSO 관련 미국 표준 문서 중의 하나인 「Chief Security Officer(CSO) Organizational Standard」(2008)에는 CSO의 핵심 책임을 다음 6가지로 정의하였다.[05]

표 1-5 CSO의 핵심 책임

핵심 책임	세부 내용
전략 개발	사업환경의 모든 위험에 대해 고위 임원들과 전략적 대응
정보 수집과 위험 평가	인력, 수익, 조직의 평판에 영향을 주는 보안 이벤트와 위협 정보를 체계적으로 수집하고 평가
조직의 준비성 확보	(물리적 또는 사이버) 공격과 재난, 보안 사고와 같이 사업의 지속성을 방해할 수 있는 사건이나 환경에 기업이 대비하도록 보증
사고 예방	사업 환경에서 보안 위험뿐 아니라 그것을 완화할 수 있는 재무적, 관리적 대책의 적용 또한 식별하고 이해해야 함, 또한 재난을 예방할 수 있는 조직 안팎의 사람들과 함께해야 함
인적 자원, 핵심 사업, 정보, 평판의 보호	회사의 무결성, 인적 자원, 프로세스, 정보, 자산이 훼손되거나 손실되지 않도록 보호

05 **저자주_** "Chief Security Officer(CSO) Organizational Standard", ASIS CSO.1-2008. 핵심 책임(key responsibility) 또는 책임이라는 표현은 해외 표준이나 글로벌 조사업체의 문서에서 자주 나오는 표현인데, 책임지는 업무라는 측면에서 그냥 업무로 해석해도 큰 무리가 없다.

핵심 책임	세부 내용
사고의 대응, 관리, 복구	공격이나 재난이 닥쳤을 경우 사고 대응과 관리, 복구 노력을 통해 핵심 시스템을 복원하고, 조직이 작동하는 데 필요한 시설을 제공

핵심 책임 중에 전략과 조직의 준비성 확보는 우리나라 법의 측면에서는 못 보던 내용이다. 또한, 정보보안을 주로 다루는 CISO와 달리 물리적 보안, 인력의 안전, 재난 대비와 같이 기업 전체의 보안과 안전을 다루고 있는 것도 눈에 띈다. 우리나라에서도 CISO는 정보 자산의 도난 방지와 같은 물리적 보안 영역까지 업무가 차츰 넓어지고 있다. 이 외에도 가트너[06]나 포레스터[07]에서 CISO의 책임(업무)을 정의한 자료가 있으니 관심 있는 분들은 참고하기 바란다.

Security Insight

CISO? CSO?

정보보호최고책임자는 CISO 즉 Chief Information Security Officer를 우리 말로 번역한 것으로, 이와 비슷한 용어로 CSO(Chief Security Officer, 최고보안책임자)가 있다. CISO가 정보 자산의 보호 또는 IT 보안을 강조하고 있다면, CSO는 IT 보안 이외에도 사옥의 물리적 보호, 기업 임직원의 안전 등 좀 더 포괄적인 보안업무를 담당하는 직책이다. 국내 문헌을 살펴보면 2006년에 고려대 정보보호대학원의 논문[08]에서 처음으로 CSO라는 표현이 나온다. 초기에는 CISO와 CSO의 역할의 차이점이 부각되었으나 정보 자산의 보호를 위해 CISO의 업무가 물리적 보안으로 차츰 넓어지면서 최근에는 CISO와 CSO를 크게 구분하지 않는 것이 추세다. 미국은 일찍부터 CSO가 생겼고, 9.11과 같은 대규모 보안 사고의 영향으로 보안 책임자의 역할이 최고위험관리책임자(CRO, Chief Risk Officer)로 확대되는 경향이 있다.[09]

06 저자주_ "Gartner for IT Leaders Overview: The Chief Information Security Officer", Gartner, July 29. 2013.

07 저자주_ "Role Job Description: Chief Information Security Officer", Forrester Research, March 5. 2012.

08 저자주_ Lauren Gibbons Paul, "Will CSOs become CROs in the future?", CSO, July 22. 2013.

09 저자주_ 정보통신서비스 제공자는 침해사고에 대한 공동 예방 및 대응, 필요한 정보의 교류, 그 밖에 대통령령으로 정하는 공동의 사업을 수행하기 위하여 제1항에 따른 정보보호최고책임자를 구성원으로 하는 정보보호최고책임자 협의회를 구성·운영할 수 있다(정보통신망법 제45조의3 제3항).

국내법에서는 주로 CISO라고 쓰고 있는데, 이것은 한국인터넷진흥원(KISA)의 위탁과제로 수행된 'CISO 제도 도입 연구'(2009.8.)라는 보고서에 기초하고 있다. 한국사회학회는 이 보고서에서 정보보호최고책임자의 명칭과 관련하여 CSO의 'S'가 Security 이외에도 Strategy, Sales, Satisfaction으로 더 많이 쓰이고, 특히 인터넷업계에서 CSO가 Chief Strategy Officer의 의미로 지칭되는 경우가 많아서 CISO라고 하는 것이 바람직하다고 기술하였다. 이 보고서가 발간되기 두 달 전에 '한국CSO협회'가 창립되어 공식적으로 CSO를 사용하는 단체가 있었으나 이 단체가 2013년 12월에 정보통신망법상의 단체인 '정보보호최고책임자협의회'로 재출범하면서[10] 국내에서는 법이나 관련 단체, 언론 매체 등에서 CSO를 공식적으로 사용하는 곳은 찾아보기 어렵게 되었다.

기업 현장에서 그리 중요할 것 같지 않은 직책 이름에 주목하는 것은 최근 논의되는 최고정보책임자(CIO)와 CISO 사이의 위상 및 역할과 관련이 있다고 보기 때문이다. 국내에서 기업 보안책임자가 정보보안뿐 아니라 기업 전체의 보안을 담당하는 CSO에서 출발했다면 정보보호 조직이 IT 조직과 분리하는 것이 굳이 쟁점이 될 만한 상황은 되지 않았을 텐데 하는 아쉬움이 있다. 도리어 CIO 산하에 CSO가 있는 것이 이상하게 보였을 것이다.

지금과 같이 CISO가 정보보안에 그 역할이 한정된다 하더라도 물리적 보안이 정보 자산을 보호하는 데 중요한 역할을 하므로 물리보안 조직이 자체 보안 정책을 수립할 때에도 CISO와 긴밀히 협의하도록 해야 보안업무가 전사 차원에서 일관성을 갖고 추진될 수 있다.

개인정보보호책임자

법에 나타난 CPO의 업무

CPO(개인정보보호책임자)나 그와 비슷한 직책을 규정한 법은 개인정보보호법, 정보통신망법, 신용정보법 세 가지가 있다. 개인정보보호법에서는 CPO의 임무를 "개인정보의 처리에 관한 업무를 총괄해서 책임"(제31조 제1항)지는 것으로 정의했다.

10 **저자주_** 신진우, 「최고보안책임관(CSO) 제도의 도입방향에 관한 고찰: 정부기관 CSO 직제의 효과적 도입 검토」, 고려대학교 정보보호대학원, 2006.2.

개인정보보호법과 그 시행령의 내용을 종합해 보면 CPO의 업무는 다음과 같다(제31조 제2항, 시행령 제32조).

표 1-6 개인정보보호법과 그 시행령에 나타난 개인정보보호책임자의 업무

제31조 제2항과 시행령 제32조	분류
1 개인정보 보호 계획의 수립 및 시행	개인정보보호 체계 수립·운영
2 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선	개인정보보호 체계 수립·운영
3 개인정보 처리와 관련한 불만의 처리 및 피해 구제	이용자의 고충 처리
4 개인정보 유출 및 오용·남용 방지를 위한 내부 통제시스템의 구축	개인정보 안전성 조치
5 개인정보 보호 교육 계획의 수립 및 시행	개인정보보호 체계 수립·운영
6 개인정보파일의 보호 및 관리·감독	개인정보 안전성 조치 개인정보 보호 체계 수립·운영
7 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행	규제 대응
8 개인정보 보호 관련 자료의 관리	개인정보보호 체계 수립·운영
9 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기	개인정보 안전성 조치
10 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치 시행	규제 대응

이는 ▲개인정보보호 체계 수립·운영(1, 2, 5, 6, 8) ▲이용자의 고충 처리(3) ▲개인정보 안전성 조치(4, 6, 9) ▲규제 대응(7, 10)으로 분류할 수 있다. CISO의 업무와 비교해 보면 전반적 업무가 유사하지만, 이용자의 고충 처리 업무가 CISO에게는 없는 업무임을 알 수 있다. 개인정보의 안전성 조치는 전형적인 CISO의 업무인데, 개인정보보호법에는 CISO 규정이 없으므로 개인정보 보호와 관련된 모든 조치의 책임은 모두 CPO에게 있다.

정보통신망법에서는 CPO의 임무를 "이용자의 개인정보를 보호하고 개인정보와 관련한 이용자의 고충을 처리"(제27조 제1항)한다고 하였다. 하지만 정보통

신망법에서는 CPO 업무를 세부적으로 규정하고 있지 않다. 다만, 법 제4장(개인정보의 보호)에서 개인정보 수집·보관·이용·제공·파기 등 개인정보 생명주기에서 이용자 동의 획득이나 개인정보의 기술적·관리적 보호조치와 같이 이용자의 개인정보 보호를 위해 사업자가 해야 할 조치들을 기술하면서 같은 장에 CPO 지정을 명시하였고, 시스템과 네트워크의 안정성을 확보하기 위해 사업자가 할 일을 규정한 제6장(네트워크의 안정성 등)에서 CISO 지정을 명시한 것으로 보아 법의 구조상 제4장(개인정보의 보호)의 조항을 CPO와 개인정보보호 조직이 할 일이라고 해석하는 것이 법의 취지와 맞아 보인다.

신용정보법에서는 신용정보관리·보호인[11]을 두도록 했는데, 그 임무를 "신용정보를 보호하고 신용정보와 관련된 신용정보주체의 고충을 처리"(제20조 제3항) 한다고 규정하였다.

신용정보법과 그 시행령에서는 신용정보관리·보호인의 업무를 다음과 같이 기술하고 있다(제20조 제3항, 시행령 제17조 제2항).

표 1-7 신용정보법과 그 시행령에 나타난 신용정보관리·보호인의 업무

제20조 제3항과 시행령 제17조 제2항	분류
1 신용정보 관리·보호 관련 내부관리규정의 제정·개정	신용정보 관리정책의 수립과 점검
2 신용정보 관리·보호 관련 고충의 처리	이용자의 고충 처리 및 점검
3 임직원이 신용정보 관리·보호 관련 법령 및 내부관리규정 등을 준수하고 있는지에 대한 점검	신용정보 관리정책의 수립과 점검

11 **저자주_** 개인신용정보는 개인정보 이외의 것을 포함하므로 엄격하게 보면 신용정보관리·보호인은 CPO에 포함되어 논의되지 않았으나 그것은 개인신용정보에 대한 사회적 관심이 적은 것에 기인하고 있고, 개인정보와 개인신용정보의 공통점과 준법감시인을 신용정보관리·보호인으로 지정할 수 있도록 한 신용정보법 시행령의 취지, 그리고 실제 대다수 금융회사에서 준법감시인이 CPO를 맡는 현실을 고려하여 이 책에서는 신용정보관리·보호인을 신용정보법상 CPO로 간주하여 설명하였다.

제20조 제3항과 시행령 제17조 제2항	분류
4 법에 따른 신용정보주체의 정당한 권리 행사에 성실하게 대응하고 있는지에 대한 점검	이용자의 고충 처리 및 점검
5 임직원을 대상으로 하는 신용정보 관리·보호 관련 교육의 실시	임직원 교육
6 그 밖에 신용정보 관리·보호에 필요한 사항으로서 금융위원회가 정하여 고시하는 사항	규제 대응

이 업무는 ▲신용정보 관리정책의 수립과 점검(1, 3) ▲이용자 고충 처리 및 점검(2, 4) ▲임직원 교육(5), 규제 대응(6)으로 요약되는데, 신용정보관리·보호인 제도가 고객의 피해 구제, 동의철회 및 전화 수신 거부, 신용정보 관련 민원 등 이용자의 고충 처리를 점검하고 감독하는 것을 핵심 업무로 출발해서 그런지 여전히 이용자의 고충 처리가 주요 업무라는 것이 눈에 띈다.[12] 2009년 신용정보법에서 신용정보관리·보호인 지정을 의무화하면서 담당 업무에 내부관리규정의 제정·개정과 그에 대한 임직원의 준수 여부 점검이 포함되어 업무가 크게 확장되었다. 내부관리규정이 신용정보 관련 각종 정책과 지침의 수립, 기술적·물리적·관리적 보안 대책의 수립 및 시행, 정보주체의 권리 보장 등 적지 않은 내용을 담은 12개의 호로 이뤄져 있기 때문이다.[13] 금융부문에서도 개인정보가 매우 중요해지면서 신용정보관리·보호인 역시 개인정보 보호책임자의 한 분류로 고려하는 추세다. 여기에서도 신용정보관리·보호인의 업무를 CPO 관점에서 해석하면 신용정보 관리정책이나 교육은 개인정보보호 체계 수립·운영으로 분류할 수 있다.

12 **저자주_** 금융감독원 신용정보실 신용정보1팀, 「금융회사 등의 개인신용정보 관리·보호 모범규준(Best Practice) 마련」, 금융감독원 정책브리핑 자료, 2005.11.8.

13 **저자주_** 신용정보업감독규정 제22조

이상 CPO의 지정과 업무를 규정하고 있는 세 법을 종합하여 재분류하면 다음 표와 같다. 표의 각 칸은 〈표 1-6〉과 〈표 1-7〉에서 해당 분류에 포함된 항목 번호다. 한 항목이 여러 분류에 포함될 수 있게 하였다.

표 1-8 관련 법에 나타난 CPO의 주요 업무 분류

분류 \ 법	개인정보보호법	신용정보법	정보통신망법	항목 수
개인정보보호 체계 수립·운영	1, 2, 5, 6, 8	1, 3, 5	N/A	8
개인정보 안전성 조치	4, 6, 9	N/A	N/A	3
이용자 고충 처리	3	2, 4	N/A	3
규제 대응	7, 10	6	N/A	3

개인정보보호는 주로 정책의 수립과 시행, 점검 등 개인정보보호 체계 수립·운영 측면에 업무의 중점이 있음을 알 수 있다. 참고로, 정보통신망법과 신용정보법에서는 CPO의 역할을 개인(신용)정보의 보호와 정보주체의 고충 처리라고 한정 짓고 있는 데 비해 개인정보보호법에서는 CPO의 임무를 개인정보의 '처리'를 총괄하고 책임지도록 광범위하게 규정하는 특징이 있다.[14]

14 **저자주_** 개인정보보호법에서는 개인정보의 '처리'를 개인정보의 "수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위"(제2조 2호)라고 하여 인터넷서비스 제공자(ISP)와 같이 개인정보를 단순 전달하는 행위를 제외하고는 거의 모든 행위를 포괄하고 있다. 즉, CPO가 개인정보 관련 모든 사항을 총괄하고 책임지는 사람으로 규정한 것이다. 하지만 실제 이 법의 제3장이나 제4장의 법 조항들은 개인정보의 처리 과정에서 해야 할 개인정보 보호업무로 한정되어 있어서 CPO의 임무를 정의한 제31조 1항의 규정은 과도한 것으로 보인다. 이 조항 역시 정보통신망법이나 신용정보법과 같이 CPO의 임무를 개인정보보호에 한정된 것으로 개정해야 하지 않을까 싶다.

CPO의 겸임

2012년 12월 말 현재 개인정보를 수집하는 5인 이상의 국내 사업체 중 CPO를 지정한 비율은 54.8%(종업원 수 250명 이상인 회사 중에서는 73.7%)이고, 그중 CPO를 전담으로 임명한 업체 비율은 28.7%에 달한다고 한다.[15] 하지만 필자가 실제로 만났거나 CPO 단체에 참여한 일정 규모 이상 기업의 CPO와 2013년 매출액 기준 30대 기업 중에서 CPO 직책을 전담한 사람은 한 명도 없었다. CISO와 같은 보안책임자가 CPO를 겸하는 경우도 포함되었다는 조사기관의 설명도 듣긴 했지만, 아마도 CPO 지정이 법적 요건이어서 법 위반의 우려 때문에 설문조사 결과가 왜곡되었을 가능성도 있지 않을까 싶다.

2014년 5월, 칼럼을 쓰기 위해 30대 기업에서 CPO의 소속을 분석해 보니 홍보부서 7곳, 경영스태프 5곳, 준법감시인 4곳, 마케팅부서 3곳, CIO(IT 부서) 3곳, HR 부서 2곳, 정보보호부서 2곳, 기타 부서 1곳씩으로 이뤄져 있었다. 겸임 조직의 성격을 살펴보면 대외활동부서(홍보·대외협력), 개인정보 이용부서(마케팅·사업), 경영스태프(경영지원·총무·경영혁신·HR·고객지원), IT 부서(CIO), 정보보호부서, 준법감시인, 감사 등으로 분류할 수 있다. 이 중에서 준법감시인이 CPO를 맡은 회사는 모두 금융회사였다. 이는 준법감시인이 금융회사나 전자금융업자에 주로 있는 직책이어서 그런 것 같다. 30대 기업에 포함된 금융회사 5곳 중 2014년 임원급 CISO를 선임한 KB국민은행은 CISO 산하의 정보보호부에서 CPO를 맡았다. 이를 소속부서의 특성을 기준으로 분류하면 다음과 같다.

---

15 **저자주_** 미래창조과학부, 한국인터넷진흥원(KISA), 「2013년 정보보호실태조사(기업부문)」, 2013.12.

표 1–9 30대 기업 CPO의 소속부서[16]

소속부서(부서, 명)	부서 특성	인원(명)
경영지원, 총무, 경영혁신, HR, 의전, 고객지원, 총무	경영스태프	9
홍보	대외활동	7
준법, 감사, 법무	내부 통제	6
마케팅, 사업본부	사업	4
CIO(IT 조직)	IT	3
정보보호	정보보호	2
합계		**31**

개인의 역량을 차치하고 소속부서 관점에서만 본다면 법에서 정의한 CPO 업무의 일부만 할 수 있는 부서에서 CPO를 맡은 것을 알 수 있다. 특히 사업본부나 마케팅부서 등 개인정보를 활용하여 사업하는 부서가 CPO를 맡은 것이 눈에 띈다. 최고경영진 입장에서는 개인정보를 많이 사용하는 부서에서 개인정보를 잘 보호하라는 지시가 합리적이라고 생각할 수도 있다. 하지만 매출 목표를 달성하기 위해 자나 깨나 고민하는 사람들은 개인정보를 보호하고 개인정보 위험을 관리하기 위해 쓸 만한 시간적, 심리적 여유가 부족하다. 또한, 개인정보의 이용과 보호 두 가치가 충돌할 때 이용 쪽에 손을 들어 줄 가능성이 농후하다. 부끄럽지만 경험담에서 나온 이야기다. 가능하면 사업부서에는 CPO를 맡기지 않는 것이 좋다.

끝으로, CPO 관련해서 한 가지 강조해 두고 싶은 게 있다. 법적으로 개인정보

16 **저자주_** 2014년 5월에 2013년 매출액 기준 30대 기업의 홈페이지를 조사한 결과이다. 30대 기업 중 삼성물산은 상사 부문과 건설 부문의 CPO가 별도로 지정되어 있어서 조사된 CPO는 총 31개이다. 개인정보보호법과 정보통신망법에 CPO에 관한 정보를 포함한 개인정보처리(취급)방침을 공개하라고 되어 있기 때문에 CPO의 지정 여부나 소속부서를 쉽게 찾아볼 수 있다.

보호의 책임은 CPO에게 있다는 점이다. 개인정보 보호조치의 핵심 내용인 관리적·기술적·물리적 보안 대책을 CISO가 담당하는 회사에서 그것이 미흡하여 개인정보 사고가 발생했다 하더라도 법적 책임은 CPO에게 있다는 이야기다. 개인정보 사고가 터진 정보통신서비스 기업에서 임원이 입건된 사례가 2번 있는데, 두 사람 모두 사고 당시 CPO였다. 다른 직책과 CPO를 겸임하는 보직자들이 많은데, 이들은 책임만 무거운 자리로 느껴질 수도 있다. 전자금융거래법의 적용을 받는 금융회사에서는 그동안 CISO의 책임이 무거웠는데, 카드사 사태 이후 신용정보법과 개인정보보호법의 적용이 강조되어서 CPO의 책임이 좀 더 강화될 것으로 보인다.

정보보호책임자의 업무

이 책은 정보보호책임자들을 위한 책이다. 이들은 기업에서 개인정보 보호(관리)책임자(CPO), 신용정보관리·보호인, 최고보안책임자(CSO), 정보보호최고책임자(CISO), 정보보호책임자 등 여러 직책을 맡고 있다. 앞에서 설명한 대로 기업에서 개인정보, 신용정보, 금융정보, 산업기밀, 의료정보, 마케팅정보, 군사정보 등을 보호하는 임무를 담당한다. 어떤 정보를 보호하든 실질적으로 기업의 중요 정보를 보호하는 책임을 진다. 말 그대로 정보보호책임자다. 이 책에서 정보보호책임자라는 용어를 선택한 첫 번째 이유다.

또한, CISO, CSO, CPO의 앞에 붙는 C는 Chief의 약자지만, 이 직책에 C레벨(C-suite) 임원을 임명하는 회사는 거의 없다고 해도 과언이 아니다. 필자도 회사에서 CEO 직속의 CSO로 일했던 1년 정도의 기간을 제외하고는 정보보

호최고책임자였지만 C 레벨 임원은 아니었다. C 레벨 임원일 때와 아닐 때의 권한이나 정보보호 조직의 위상, 그에 따른 업무 추진에서 상당한 차이가 있다. CISO나 CPO의 'C'를 강조하면 이 직책의 권한을 과도하게 이해하여 현실과 유리된 정책이나 주장을 펴기에 십상이다. 이것이 정보보호책임자라는 용어를 선택한 두 번째 이유다.

기업에는 임원이나 본부장급은 아니지만, 명목상 CISO나 CPO가 있든 없든 팀장이나 차·부장급 중에서 실질적인 정보보호 '책임자' 역할을 하는 사람이 상당수 있다. 임직원이 수천 명이 넘는 대기업에서도 그런 경우를 본다. 이들 역시 이 책에서 말하는 정보보호책임자다.

앞에서 살펴본 정보보호 업무 또는 정보보호 조직의 업무는 정보보호책임자가 책임지고 진행하는 일이다. 정보보호 대책 구현같이 정보보호책임자가 최종 책임을 지는 업무가 있지만, 정보보호 조직의 구성과 예산 확보같이 정보보호책임자가 수행 책임을 지고, 최종 책임은 CEO나 CFO 등 최고경영진에게 있는 업무도 있다.

이 책에서는 정보보호책임자의 임무를 "기업의 경영목표 달성을 위한 전사 정보보호 전략의 수립과 실행"이라고 정의한다. 경영목표를 달성하기 위해 회사와 사업의 보안 위험을 줄이는 게 핵심적인 업무다. 정보보호책임자가 사업의 성격과 전사적인 목표를 모두 꿰고 그것에 영향을 미치는 보안 위험 요인과 그에 대한 대책을 세워야 한다. 그래야 CEO를 비롯한 최고경영진이 정보보호책임자가 자신과 동떨어진 업무를 수행하는 사람이 아니라 자신들의 목표를 위해 꼭 필요하고 최선을 다하는 사람으로 인식하게 된다.

그러기 위해 정보보호책임자가 해야 할 일을 5가지 영역, 24가지 업무로 정리

하였다. 앞에서 살펴본 법과 해외 표준을 고려하고, 정보보호의 국제적인 흐름과 국내 기업의 정보보호책임자들이 실제로 고민하는 사항을 담았다.

표 1-10 정보보호책임자의 업무[17]

영역	업무	세부 내용
1 거버넌스	1 이사회·경영진 주도 체계 구축	- CEO를 비롯한 최고경영진이 보안 위험을 책임지고 주도하는 체계 구축과 전사적인 커뮤니케이션 시행 - 임원급 (전담) 정보보호책임자 선임과 위상 부여
	2 경영진 및 타 임원 소통 체계 구축	- 주요 임원이 정보보안 정책 등 정보보호 관련 의사결정, 전략 및 정책 공유, 전사적인 추진과 협업할 수 있는 체계 구축 - 임원회의, 정보보호 경영위원회에서 정보보호 의제 처리와 소통
	3 정보보호 조직·인력·예산 확보	- 정보보호 조직의 구축과 위상 확보 - 적절한 규모의 보안 인력 및 보안전문가 - 정보보호 예산 확보
	4 정보보호 계획의 수립과 추진	- 회사 경영목표와 연계된 정보보호 전략 및 사업계획 수립. 전사 관련 조직의 정보보호 활동이 각 조직의 사업계획에 포함되도록 협업 - 회사 경영목표 달성에 잠재한 정보보안 위험의 최소화
	5 정보보호 경영 지원	- CEO의 정보보호 어젠더 지원 - 정보보호책임자의 정보보호 어젠더 수립과 추진 - 타 임원의 정보보호 업무 및 활동 지원
2 관리 체계	1 보안 위험 관리	- 정보 자산의 식별, 보호대상 자산의 선정 - 보안 위험의 식별, 보안 취약점 및 보안 위험의 분석 관리 - 정보보호 대책의 수립과 이행 관리 - 정보보호 아키텍처 설계 및 관리
	2 정보보호 정책 수립·관리	법규를 반영하고, 보안 위험을 완화하며, 회사의 현실을 고려한 정보보호 정책과 지침 및 프로세스의 수립과 관리

17 **저자주_** 제4절(개인정보보호책임자)에서 살펴본 CPO의 업무 중 이용자의 고충 처리 업무는 이 표에서 제외하였다. 이 업무의 법적 책임은 CPO에게 있으나 대부분 기업에서는 고객센터에서 이 업무를 처리하기 때문에 제외해도 정보보호책임자의 업무를 기술하는 데에 별 무리가 없다고 판단하였다.

영역	업무	세부 내용
	3 협업 관리	- 타 임원 및 부서장과의 소통을 통해 정보보호 조직의 전사 정보보안 정책 및 업무 추진, 협업 지원 - IT 부서 및 비IT 부서와의 협업 - 전 부서의 적절한 정보보호 담당자 선정을 통한 정보보호 실무위원회의 구성과 운영, 의욕 관리, 이점 제공
	4 정보보호 교육 및 인식 제고	임원·직책자·일반 구성원의 정보보호 교육, 생활 보안 점검, 보안 캠페인 등을 통한 인식 제고
	5. 보안 감사	정보보호 정책과 지침, 프로세스가 회사의 정책대로 수행되고 있는지 사내 및 관계사와 협력업체 등을 점검하고 결과에 따라 적절하게 상벌할 수 있는 제도의 수립 및 운영
	6 정보보호 조직 관리	- 정보보호 조직의 업무 추진 고충 해결과 대책 지원 - 정보보호 인력의 동기부여, 육성, 경쟁력, 자발성 제고 - 보안 운영 외주직원 관리
3 중요 자산 보호	1 정보보호 시스템 구축	- 도입, 개발(외주, 내부) 등을 통한 정보보호 시스템 구축 및 세부 룰 설정 - 정보보호 시스템 계정, 접근 권한, 접근 통제 등 정보보호 시스템의 보호를 위한 정책 설정
	2 정보보호 시스템의 운영·점검·개선	- 정보보호 시스템과 관련 프로세스 운영 - 로그, 룰 현황을 정기적으로 보고받기 - IT 인프라 및 애플리케이션의 변경, 새로운 보안 위협의 등장, 룰의 누적, 담당 인력의 변화 등에 대한 분석 및 개선
	3 모니터링, 탐지, 대응	- 외부 침입 및 정보 유출 탐지를 위한 보안관제 운영 - 내부 통제, 이상 징후 시스템 등의 모니터링과 탐지, 후속 조치
	4 IT 인프라 및 IT 개발의 보안 정책 수립·점검	IT 인프라의 보안, 계정 및 접근 권한 관리, 사용자 인증, 접근 통제, 제품·서비스·애플리케이션의 개발 보안, 데이터 암호화 등 IT 관련 보안 정책 및 프로세스의 수립·점검
	5 비IT 보안 정책의 수립·점검	인적 보안, 외주 계약 및 관리, 비고객 개인정보 관리(HR·IR 부서 등), 구매관리, 출입통제, 제품보안 등 비IT 보안 업무에 대한 정책과 프로세스의 수립 및 점검
4 위기관리	1 정보보호 위기 대응 정책 및 프로세스 수립	정보보호 사건·사고·위기에 대한 대응 정책, 조직, 프로세스의 수립과 운영

영역	업무	세부 내용
	2 업무 연속성 계획 수립·운영	IT 재해복구 대책 등 업무 연속성 계획 수립, 필요 인력과 시설 확보 및 운영
	3 위기 대응 모의훈련	피싱 메일, 디도스(DDoS) 공격, 침해사고, IT 재해 등에 대한 비상 대응 훈련
	4 보안 이슈 및 위기 대응	각종 정보보호 사고 및 SNS 유포 등 일상적 보안 이슈 대응, 정보보호 위기 대응
	5 외부 협력 구축과 운영	정보보호 단체 참여, 정보보호 자문위원회 운영 등을 통해 위기 대응 사전 준비
5 규제 대응	1 대내외 규제 분석 및 준수 점검	- 적용 법규(법, 시행령, 시행규칙, 고시), 안내서, 해설서 등의 파악과 회사 관련 부분 분석, 사내 준수 점검 - 관련 법규의 변화 관리
	2 대내외 규제기관 대응	- 외부 규제기관과 수사기관 대응, 그룹 또는 모기업의 요구 및 보안 점검 대응 - 내부 통제 및 외부 감사 대응
	3 정보보호 인증 획득 및 유지 관리	정보보호 관련 인증 획득 및 유지 관리(보안 감사와 연계 가능)

〈표 1-10〉을 보면 앞에서 살펴본 법이나 표준과 달리 거버넌스 영역의 업무가 많다. 앞에서 분석한 법과 표준들도 세부적으로 들어가면 거버넌스 영역의 업무를 포함하긴 하지만, 여기서는 거버넌스 업무를 정보보호책임자가 수행해야 할 핵심 업무 영역의 하나로 분류했다. 최근 보안 위험이 회사 전체의 위험이 되면서 결국 재무 위험이나 법규 위험같이 최고경영진이 다뤄야 할 위험이 되었다고 보기 때문이다. 정보보호의 국제적인 흐름에서도 거버넌스의 중요성이 강조되고 있다. 정보보호 거버넌스는 정보보호 활동이 전사적으로 영향을 미치기 위한 기반이 된다. 거버넌스 업무는 정보보호책임자가 수행해야 할 중요한 업무이긴 하지만, 정보보호책임자가 책임지고 추진하기에는 한계가 있는 업무이기도 하다. 세부 업무를 살펴보면 '정보보호 경영지원(1-5)' 업무를 제외하

고는 최고경영진이 주도적으로 추진하거나 최종 승인하여 정보보호책임자에게 힘을 실어 줄 때 가능한 업무들이다.

관리 체계 영역의 업무는 기업의 보안 관리를 위한 체계를 갖추고 운영하는 업무다. 이 체계가 잘 갖춰져 있으면 실무적인 정보보호 업무는 무리 없이 돌아간다. 정보보호책임자는 관리 체계 영역 업무들의 최종책임자로서 관리 포인트를 갖고 들여다보고 관리 및 개선해 나가면 된다. 특히 보안 위험 관리(2-1) 업무는 사업과 사업목표 달성에 위험이 되는 보안 위험을 찾아내고 줄여나가기 위한 출발점이 되는 업무이다. 개인정보 유출, 서비스 중단, 시스템 파괴뿐 아니라 매출 감소, 법적 위험 등을 종합적으로 고려할 필요가 있다. 또한, 협업 관리(2-3)는 전사의 각 부서가 수행해야 할 정보보호 업무를 관리하기 위해 필수적인 업무다. 겉으로 잘 드러나지는 않지만, 정보보호책임자가 반드시 해야 할 일이어서 별도 업무로 뽑았다.

중요 자산 보호 영역은 한마디로 하면 정보보호 사고가 발생하지 않게 하는 업무들로 구성된다. 전통적으로 정보보호 조직의 업무인 관리적·기술적·물리적 보안 대책을 세우고 그것을 구현·운영·개선함으로써 보안 공격을 차단하거나 탐지·대응하여 보안 사고를 예방한다. 정보보호 조직의 일상적인 업무 대부분이 여기에 속한다. 앞에서 식별한 보안 위험 및 보안 사고와 직접 연결되는 취약점을 찾아 없애는 게 관건이다.

이제까지 많은 중요 자산의 업무가 IT 영역에 집중되어 있는데, IT 부서 외에서 수행하는 정보보호 업무를 잘 들여다보고 관리해 나갈 수 있어야 한다. 최근 문제가 된 외주관리 보안이나 출입통제 같은 물리 보안도 역시 정보보호책임자가 잘 챙겨야 보안 위험을 줄일 수 있다. 정보보호책임자가 세부적인 내용을 다

알기는 어렵다 하더라도 각 업무의 핵심적인 관리 포인트를 이해하면 업무를 보고받고 질문하면서 목적에 부합하게 수행되고 있는지를 점검할 수 있다.

위기관리 영역의 업무는 개인정보 유출 사고와 같은 큰 사고뿐 아니라 기업 내에서 소소하게 발생하는 정보보호 사건·사고가 정보보호 위기로 번져 나가지 않도록 신속하게 대응하고, 정보보호 위기가 발생했을 때를 대비해 사전에 준비하며, 실제 위기가 발생하면 전사적인 위기 대응 활동으로 회사의 손실을 최소화할 수 있도록 하는 업무다. 그러기 위해 모의훈련 등 사전에 준비해야 할 일들이 있다.

규제 대응 영역의 업무는 정보보호 관련 법과 행정 규제, 기업의 정보보호 정책이나 지침과 같은 자체 규제, 여론과 시민단체 등에 의한 사회적 규제에 대응하는 업무다. 당장 별도로 분리할 만큼 정보보호책임자가 담당할 업무가 많지 않을 수도 있다. 하지만 2014년을 기점으로 예방적 규제가 강화되었을 뿐 아니라 결과의 책임을 묻는 규제까지 추가되면서 정보보호 규제로 인한 기업의 위험은 매우 커졌다. 정보보호책임자가 반드시 관리해야 할 영역이다.

이 책에서는 24가지 업무를 각각 다루기보다는 영역별로 핵심이나 유의해야 할 사항을 중심으로 포괄적으로 기술한다. 24가지 업무에는 정보보호책임자가 직접 실행해야 하는 업무도 있지만, 정보보호 조직이나 IT 조직이 실무적으로 처리해야 할 업무도 상당히 포함되어 있다. 후자의 업무는 정보보호책임자가 그것의 수행 책임이나 최종 책임을 갖게 되므로 그 업무의 스토리를 이해하고 통찰을 갖고 관리 포인트를 짚는다면 큰 무리 없이 업무를 소화할 것으로 판단된다. 2장부터 기술된 내용을 이런 관점에서 읽어 주기 바란다.