KBR 제28권 제1호 2024년 2월 http://dx.doi.org/10.17287/kbr.2024.28.1.49

정보보호최고책임자의 겸직과 정보보호 성과: 정보보호 공시 데이터를 중심으로*

최 돈 수**
김 태 성***

2012년 2월에 개정된 『정보통신망법』에서 정보보호최고책임자(Chief Information Security Officer, CISO)의 임원급 지정 제도를 도입했다. 그러나 10여 년이 지난 현재도 많은 공공기관 및 민간기업에서는 CISO의 필요성을 인식하지 못하거나, 다른 최고책임자(Chief X Officer, CXO)가 CISO의 업무를 겸직하여 CISO의 업무를 충분히 수행하지 못하는 경우가 많다.

본 연구에서는 정보보호 공시 자료를 제출한 기업들의 데이터를 분석하여 CISO의 겸직 여부에 따라 정보보호 인증 취득에 미치는 영향을 조사하고, 겸직 여부에 따라 정보보호 투자액과 정보보호 인력규모에도 차이가 있는지를 조사한다. 또한, 겸직 비율이 높은 CXO를 조사하여 이들의 업무와 차이점을 구별하고, 겸직 시 문제점에 대해 분석하는 것을 목적으로 한다. 이를 통해 기업은 적절한 역할 분담과 역할 및 책임의 명확한 정의 등을 고려하여 정보보호를 강화하는 데 도움이 될 것으로 기대된다.

주제어: CISO, Dual Position, Information Security Performance, Information Security Disclosure, CXO

Ⅰ. 서 론

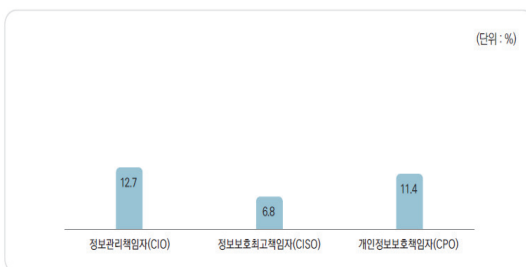
최근 몇 년 동안 급격한 디지털화와 COVID-19 팬데믹으로 인해 원격 근무 등 새로운 업무 방식이 증가함에 따라 정보보안의 중요성이 더욱 부각되고 있는 가운데 정보보안 침해 및 유출 사고는 매년 꾸준하게 증가하고 있다. 이러한 정보보안 위협으로부터 기업의 비즈니스 연속성을 유지하는 것은 매우 중요한 과제이며, 이런 과제에 대한 정책을 올바르게 수립하는 역할을 할 수 있는 책임자가 바로 정보보호최고책임자(Chief Information Security Office, 이하 CISO)다. 2012년 2월 『정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하, 정보통신망법)』에서 CISO의 임원급 지정 제도가 신설된 이후. 2014년 1월 카드사 개인정보 대량 유출사건이 발생하면서 CISO의 겸직 문제에 대한 이슈가 더욱 두드러졌다. 금융권을 중심으로 CISO의 겸직을 제한하는 조항이 처음으로 『전자금융거래법』에 도입되었고, 이후 2018년 6월 『정보통신망법』에서도 CISO의 겸직 제한이 신설되어, 이 조항은 금융권뿐만 아니라 다양한 기업에 적용되었다〈표 1〉.

〈표 1〉 CISO 관련 법 신설 시기

시기	2012년 2월	2014년 10월	2018년 6월
법	정보통신망법	전자금융거래법	정보통신망법
내용	CISO 임원급 지정 신설	CISO 겸직 제한 (CIO 대상)	CISO 겸직 제한(전체)

논문접수일: 2023. 09. 04. 1차 수정본 접수일: 2023. 11. 22. 2차 수정본 접수일: 2023. 12. 31. 게재확정일: 2024. 01. 09
* 이 논문은 2022학년도 충북대학교 연구년제 지원에 의하여 연구되었음
** 충북대학교 융합보안협동과정 석사과정(cds0104@naver.com), 제1저자
*** 충북대학교 경영정보학과 및 융합보안협동과정 교수(kimts@cbnu.ac.kr), 교신저자

그러나, 법으로 제한을 하고 있음에도 기준에 해당되지 않는 많은 공공기관 및 민간 기업에서는 아직까지 CISO를 지정하지 않고 있으며, 예산이나 내부 조직 구조 등으로 인해 CISO의 업무를 다른 최고책임자(Chief X Officer, 이하 CXO)가 겸임하여 CISO의 업무를 제대로 수행하고 있지 않거나 업무 우선순위가 후순위로 밀려있는 경우가 많다. 또한, 이런 기업들 중에는 CISO의 필요성을 전혀 깨닫지 못하고 있는 기업들도 많다. 2021년 정보보호 실태조사 자료에 따르면 국내 사업체에서 CISO를 임명한 비율은 6.8%에 불과하며 이는 정보관리최고책임자(Chief Information Officer, 이하 CIO) 12.7%, 개인정보보호책임자(Chief Privacy Officer, 이하 CPO) 11.4%에 비해 상당히 미흡한 수치다〈그림 1〉.



(출처: '2021 정보보호실태조사' 과학기술정보통신부, 한국정보보호산업협회)

〈그림 1〉 CIO, CISO, CPO 임명률

이에 따라 본 연구에서는 정보보호 공시 자료를 제출한 기업들의 데이터를 분석하여 CISO의 겸직 여부에 따라 정보보호 인증 취득에 미치는 영향을 조사하고, 겸직 여부에 따라 정보보호 투자액과 정보보호 인력규모에도 차이가 있는지를 조사한다. 또한, 겸직 비율이 높은 CXO를 조사하여 이들의 업무와 차이점을 구별하고, 겸직 시 문제점에 대해 분석하는 것을 목적으로 한다. 이를 통해 기업은 적절한 역할 분담과 역할 및 책임의 명확한 정의 등을 고려하여 정보보호를 강화하는 데 도움이 될 것으로 기대된다.

II. 이론적 배경

2.1 CISO의 정의와 역할

CISO는 기업 내에서 정보보안을 총괄하는 최고책임자이다. CISO는 조직의 정보 자산을 보호하고 사이버 위협으로부터의 공격을 예방하며, 조직의 정보보안 전략과 정책을 개발하고 관리하는 역할을 맡는다. 또한, CISO는 전략적 사고, 정보보안 정책 및 절차 개발, 사이버 위협 대응, 리스크 관리, 커뮤니케이션 및 협력 등과 같은 역할을 수행함으로써 조직의 정보보안을 강화하고 사이버 위협으로부터의 공격을 예방하며, 비즈니스 운영에 필수적인 안전성과 신뢰성을 보장한다. 또한, 기업의 IT 자산에 대한 해킹 및 바이러스 등의 공격에 대비하기 위해 적합하고 효율적인 정보보호 솔루션을 도입하여 기업 내·외부에서의 공격에 대응할 수 있도록 대비하는 것도 CISO가 담당해야 할 역할이다.

이에 따라 기업이나 조직에서는 CISO를 중요한 직무로 인식하고 있으며, CISO의 수요 또한 증가하고 있지만, 여전히 많은 공공기관 및 민간기업에서는 CISO의 중요성을 인식하지 못하고 있다. Karanja & Rosso(2017)와 Kotulic & Clark(2004)는 CISO의 위치에 대한 학술 연구 문헌은 거의 없다고 주장하였으며, Ashenden & Sasse(2013)는 현재 많은 대기업에서 CISO를 두고 있지만, 그에 대한 연구는 제한적이고 CISO의 권한 부족, 역할 정체성에 대한 혼란, 직원을 효과적으로 참여시킬 수 없는 능력으로 인해 신뢰를 얻기가 어렵다고 주장하였다. CISO의 보고 체계에 관한 연구도 많이 진행되었는데, Karanja & Rosso(2017)는 CISO의 역할 또는 CIO와 CISO의 관계가 IT보안 자원에 어떠한 영향을 미칠 수 있는지 연구하기 위해 Hardy(1996)의 조직의 힘, Eisenhardt(1989)의 대리인 이론을

참조하여 조사한 결과, CISO와 CEO의 직접 보고 체계가 성립되지 않고 CIO를 통한 간접 보고 체계가 성립될 경우 보안 취약성이 은폐될 수 있으며, 이를 악용할 경우 소송 및 비즈니스 손실이 발생할 수 있다고 하였다. Kayworth & Whitten(2010), Baskerville & Dhillon(2008), Ashenden(2008) 등의 연구는 CISO-CEO의 보고 구조를 상세하게 분석하였으며, 이러한 직접 보고 체계는 CEO 또는 이사회 구성원 간의 커뮤니케이션 격차를 최소화한다고 하였다.

CISO와 관련된 선행연구 검토 결과, 아직까지도 CISO의 중요성이 부각되지 않아 연구가 부족하며, CISO의 위치 및 보고체계, 업무가 명확하지 않았음을 확인하였다.

2.2 『정보통신망법』에 명시된 CISO의 겸직 업무

『정보통신망법』 제45조의3제4항에서는 CISO의 업무와 겸직 시 수행해야 할 업무에 대해 명시하고 있다. 명시된 CISO의 업무는 〈표 2〉와 같다.

〈표 2〉 정보통신망법 제45조의3 4항 1호

가. 정보보호 계획의 수립·시행 및 개선
나. 정보보호 실태와 관행의 정기적인 감사 및 개선
다. 정보보호 위험의 식별 평가 및 정보보호 대책 마련
라. 정보보호 교육과 모의 훈련 계획의 수립 및 시행

또한, 『정보통신망법』에서 정의된 CISO를 겸직 시 수행해야 할 업무는 〈표 3〉과 같다.

본 논문은 CISO의 겸직과 관련된 내용을 조사하고 있기 때문에 〈표 2〉에 해당되는 겸직 시 수행해야 할 업무에 대해 살펴보았다. '가.', '나.', '다.' 목의 경우 업무가 상이하긴 하지만, 모두 CISO의 업무였고, 다른 CXO와 겸직이 가능한 부분은 '라.' 목을 통해 확인이 가능하다. 해당 목에서는 CPO의 업무에 해당되는 개인정보 업무가 포함되어 있었으며, 내용은 〈표 4〉와 같다.

〈표 3〉 정보통신망법 제45조의3 4항 2호

가. 『정보보호산업의 진흥에 관한 법률』 제13조에 따른 정보보호 공시에 관한 업무
나. 『정보통신기반 보호법』 제5조제5항에 따른 정보보호책임자의 업무 『전자금융거래법』 제21조의2 제4항에 따른 정보보호최고책임자의 업무
다. 『전자금융거래법』 제21조의2제4항에 따른 정보보호최고책임자의 업무
라. 『개인정보 보호법』 제31조제2항에 따른 개인정보 보호책임자의 업무
마. 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행

『정보통신망법』에서의 겸직 제한은 자산 총액, 정보보호 관리체계(ISMS) 의무 대상 기업에 국한되어 있으나, 해당 기업들의 CISO와 겸직 가능한 CXO 및 CXO의 업무가 법에 별도로 명시되어 있지 않고, 모두 CISO 업무인 정보보안과 관련된 업무만 기재되어 있었다. 단, CPO의 업무에 해당되는 개인정보 업무는 겸직이 허용되어 있음을 확인하였다.

〈표 4〉 개인정보 보호법 제31조 2항

1. 개인정보 보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보 보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리·감독
7. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무

Ⅲ. 정보보호공시기업 조사 및 분석

3.1 정보보호공시제도의 개요

디지털 전환 과정에서 발생하는 사이버 침해사고, 디지털 대란 등이 기업의 경제적 피해, 대외 신뢰도 저하, 이용자 불편 등 기업 경영에 직·간접적인 영향을 끼치게 됨에 따라, 정보통신서비스 관련 기업뿐 아니라 이용자의 개인정보를 대량으로 보유한 전자상거래 기업 또는 중요 연구개발 정보를 보유한 첨단기업, 사회 기반시설 등 모든 기업에 정보보호가 핵심 경쟁력으로 부각되었다. 그러나 기업의 정보보호 현황은 위험관리와 관련된 주요 정보이지만 그동안 시장에서 투명하게 공개되지 못하였으며, 이해관계자들은 해당 기업의 정보보호 현황을 알 수 없어 불충분한 정보로 서비스 이용, 투자 등 의사결정이 이루어졌으며, 이에 따라 이용자 보호 및 알 권리를 보장하고 기업의 자발적인 정보보호 투자를 촉진하기 위해 정보보호 공시제도를 만들게 되었다.

정보보호공시제도는 2016년부터 자율공시 제도로 시행되었으며, 2021년 국회가 정보보호 투자 활성화 및 이용자보호를 위하여 『정보보호산업법』을 개정하면서 2022년부터 정보보호 공시 의무제도가 시행되었다. 2016년 2개 기업을 시작으로 2022년에는 의무공시 및 자율공시를 포함하여 648개(2022년 11월21일 기준이며, 2022년 12월 31일 기준 660개) 기업이 정보보호 공시 이행을 완료하였다〈표 5〉.

정보보호공시제도의 적용 대상으로는 『정보보호산업법』 제13조제2항에 따라 의무자로 지정되는 의무공시 대상과 그 밖에 정보통신망을 통하여 정보를 제공하거나 정보의 제공을 매개하는 자에 한 해 자율공시 대상이 있다.

의무 공시 대상은 사업분야, 매출액, 이용자 수의 항목 중에 하나라도 기준에 해당되면 의무 공시 대상이 된다. 사업분야로는 『전기통신사업법』 제6조제1항에 의한 회선설비 보유 기간통신사업자, 『정보통신망법』 제46조에 의한 집적정보통신시설 사업자, 『의료법』 제3조의4에 의한 상급종합병원, 『클라우드컴퓨팅법』 시행령 제3조제1호에 의한 클라우드컴퓨팅 서비스제공자가 해당되며, 매출액으로는 CISO를 지정·신고하여야 하는 유가증권시장 및 코스닥시장 상장법인 중 매출액 3,000억 원 이상이 해당된다. 이용자 수는 정보통신서비스 일일 평균 이용자 수 100만 명 이상(전년도 말 직전 3개월간)이 의무공시 대상에 해당된다. 여기서 이용자 수는 순방문자 수(IP 기준 1일 방문자 수)를 의미한다.

〈표 5〉 연도별 정보보호 공시 이행 현황

연도	2016	2017	2018	2019	2020	2021	2022
자율공시	2	10	20	30	45	64	62
의무공시	-	-	-	-	-	-	586
합계	2	10	20	30	45	64	648

* 정보보호 공시 종합 포털, 2022 정보보호 공시 현황 분석보고서 참조

공시 의무 제외 대상으로는 공공기관, 소기업, 금융회사, 전자 금융업자가 해당된다. 공공기관은 『공공기관운영법』에 의한 공기업 및 준정부기관 등이 해당되며, 소기업은 『중소기업기본법 시행령』 제8조제1항에 의한 평균 매출액 120억 원 이하 기업이 해당되나, 업종별 매출액 기준이 상이하며(10~120억 원), 정보통신업은 50억 원 이하가 해당된다. 금융회사의 경우 『전자금융거래법』 제2조제3호에 의한 은행, 보험, 카드 등 금융회사가 해당되며, 전자 금융업자로는 『전자금융거래법』 제2조제4호 및 한국표준산업분류에 의한 정보통신업 또는 도·소매업을 주된 사업으로 하지 않는 전자금융업자가 해당된다.

정보보호공시제도 공시 항목으로는 정보보호 투자 현황, 정보보호 인력 현황, 정보보호 관련 인증·평

가・점검 등에 관한 사항, 정보통신서비스를 이용하는 자의 정보보호를 위한 활동 현황 4가지 항목별로 내용을 기재하여 최고경영자 확인을 받는데, 3.2절에서 조사한 내용에 해당되는 CISO 겸직 현황은 정보보호 인력 현황 항목에서 확인할 수 있다.

3.2 정보보호공시기업 CISO 겸직 관련 조사 및 분석

본 연구는 CISO의 겸직 현황을 조사하기 위해 정보보호 공시 종합 포털 사이트를 활용하여 정보보호 공시기업을 대상으로 겸직 현황을 조사하였다. 2022년도에 정보보호 공시 종합 포털 사이트에 공시한 기업은 총 660개였으며, 해당 기업들을 대상으로 IBM SPSS Statistics 24를 활용하여 데이터의 분석을 수행하였다. 그 결과 CISO를 겸직하는 기업은 총 468개로 전체의 70.91%로 조사되었다. 해당 결과를 기초 데이터로 활용하여, CISO 겸직 여부에 따른 정보보호 인증 취득여부 및 정보보호 인증 종류별 취득여부 차이, 정보보호 투자액, 정보보호 인력에 영향을 미치는지 비교하였다. 이를 통해 CISO의 겸직이 미치는 영향을 다양한 측면에서 심층적인 분석을 실시하였다.

3.2.1 CISO 겸직과 정보보호 인증의 인과관계 분석

일반적인 기업에서 정보보안 수준이 높다는 것을 증빙하기 위해 정보보호 인증을 취득하며, 정보보호 인증을 받은 기업은 대외적으로 정보보호 강화에 시간과 노력을 투자하고 있다는 것으로 인정된다. 국내 정보보호 관리체계 인증인 ISMS(ISMS-P) 인증을 취득한 기업은 인증을 취득하지 않은 기업에 비해 연간 2억2천만 원의 비용을 절감하고 있는 것으로 나타났다(고규만, 2010). 그만큼 정보보호 인증 취득은 정보보호 성과를 높이는데 중요한 부분을 차지한다. 국내에서 가장 많이 취득하는 정보보호 인증은 ISMS, ISMS-P, ISO27001 세 가지이다. ISMS는 정보보호 중심인 80개의 세부심사항목으로 인증하는 국내 정보보호 인증이며, 일정한 기준에 부합하는 기업은 강제적으로 취득하도록 되어 있다. ISMS-P의 경우는 ISMS의 80개의 세부심사항목에 개인정보보호 항목 22개가 추가적으로 더해져 102개 항목을 심사하는 정보보호 인증이다. ISMS-P는 ISMS와 달리 강제성이 없으며, 기업에서 자율적으로 취득할 수 있다. ISO27001은 정보보호 중심의 114개의 세부 심사항목으로 인증하며, 국제 정보보호 인증으로 해당 인증 또한 ISMS-P와 동일하게 강제성 없이 자율적으로 취득하며, 국제 표준으로 국외에서 정보보호 분야로 가장 권위 있는 국제 인증이다.

CISO의 겸직 여부에 따라 기업이 정보보호 강화에 투자를 하고 있는지 비교하기 위해 정보보호 인증 취득 여부를 통해 확인하였다. CISO의 겸직 여부가 정보보호 인증 취득 여부에 영향을 미치는지 이항 로지스틱 회귀분석을 통해 조사하였으며〈표 6〉, CISO를 겸직하지 않는 경우 '1'의 값, 겸직하는 경우 '0'의 값을 갖는 독립변수로 설정하고, 정보보호 인증을 취득했을 경우 '1'의 값, 취득하지 않았을 경우 '0'의 값을 갖는 종속변수로 설정하여 해당 종속변수와 독립변수를 이항변수로 설정하였다. 정보보호 인증의 경우 ISMS, ISMS-P, ISO27001 세 개의 정보보호 인증 중 하나라도 취득하였을 경우를 인증을 취득한 것으로 분류하여 분석을 수행하였다.

분석 결과, 정보보호 인증을 취득하고, CISO를 겸직하지 않았을 때의 경우 계수(B)는 0.877, 계수의 지수값(Exp(B))이 2.403으로 확인되어 계수(B)가 양수이므로 CISO를 겸직하지 않을 경우 정보보호 인증을 취득할 가능성이 증가하며, 계수의 지수값(Exp(B))이 2.403으로 1보다 크므로 정보보호 인증을 취득할 확률이 2.403배로 높아지는 것으로 나타났다. 해당 결과들의 유의성 검정은 유의확률(p-value), 표준오차(S.E.), 왈드 통계량(Wald)로

확인하였으며, 유의확률(p-value)은 일반적인 0.05 이하 값을 기준으로 보다 작은 값인 0.000으로 나타나 통계적으로 유의미한 것으로 확인되었고, 회귀 계수의 추정치의 정확성을 나타낸 표준오차(S.E.)의 경우 값이 작을수록 정확성이 높아지는데, 0.175의 작은 값으로 나타나 정확성이 높게 나왔으며, 회귀 계수의 유의성을 평가하는 왈드 통계량(Wald)의 경우는 높은 값일수록 유의미한 계수를 나타내는데, 25.045의 높은 값을 나타내어 유의미한 계수임을 확인하였다.

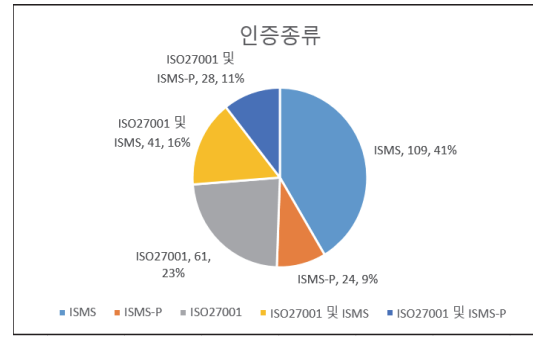
따라서, 해당 결과는 CISO 겸직 여부와 인증 취득 여부 간의 유의한 관계를 보여주어, 기업에서 CISO를 겸직하지 않을 때 정보보호 인증 취득을 적극적으로 추진하는 것을 확인할 수 있다.

〈표 6〉 CISO 겸직과 정보보호 인증 취득의 인과관계

종속변수	독립변수	계수(B)	표준오차(S.E.)	왈드 통계량(Wald)	자유도	유의확률(p-value)	계수의 지수 Exp(B)
정보보호 인증 여부	겸직 여부	0.877	0.175	25.045	1	0.000	2.403

다음으로, 정보보호 인증 취득 종류 별로 다중 분석을 통해 빈도를 조사하였다. 정보보호 인증을 받은 기업의 총 수는 263개로, 이중 ISMS 인증을 받은 기업의 수는 109개(41.4%), ISMS-P 인증을 받은 기업의 수는 24개(9.1%)이다. 또한, ISO27001 인증을 받은 기업은 61개(23.2%), ISMS와 ISO 27001을 모두 받은 기업은 41개(15.6%), ISMS-P와 ISO27001을 모두 받은 기업은 28개(10.6%)로 확인되었다〈그림 2〉.

또한, CISO 겸직 여부가 정보보호 인증 종류별 취득에 어떠한 영향을 미치는지 이항 로지스틱 회귀분석을 통해 조사하였다. CISO를 겸직하지 않는 경우 '1'의 값, 겸직하는 경우 '0'의 값으로 독립변수로



〈그림 2〉 정보보호 인증 종류별 건수

설정하였고, 정보보호 인증 별(ISMS, ISMS-P, ISO 27001, ISO27001 및 ISMS(중복 인증), ISO27001 및 ISMS-P(중복 인증))로 취득했을 경우 '1'의 값, 취득하지 않았을 경우 '0'의 값으로 종속변수로 설정하여 각각 별도로 이항 로지스틱 회귀분석을 실행하였다.

분석 결과, ISMS-P, ISO27001, ISO27001 및 ISMS, ISO27001 및 ISMS-P의 인증을 받은 경우 계수(B)가 각각 1.112, 0.894, 1.450, 1.095, 계수의 지수값(Exp(B))이 각각 3.041, 2.445, 4.264, 2.990으로 나왔다. ISMS-P, ISO27001, ISO27001 및 ISMS, ISO27001 및 ISMS-P의 인증을 받은 경우 계수(B)가 양수이므로 CISO를 겸직하지 않을 경우 해당 정보보호 인증을 받을 가능성이 증가한다는 것을 의미하며, 계수의 지수값(Exp(B))이 1보다 크므로 해당 인증들을 받았을 경우 겸직하지 않을 확률이 각각 3.041배, 2.445배, 4.264배, 2.990배로 높아짐을 의미한다.

ISMS 인증을 받은 경우에는 다른 인증들의 결과와 다른 결과를 보였다. 계수(B)가 -0.495, 계수의 지수값(Exp(B))이 0.610으로 나와 CISO를 겸직하지 않았을 때 ISMS 인증을 받은 경우 계수(B)가 음수이므로 CISO를 겸직하지 않을 경우 ISMS 인증을 받을 가능성이 감소한다는 것을 의미하며, 계수의 지수값(Exp(B))이 1보다 작으므로 ISMS 인증이 1 증가할수록 겸직하지 않을 확률이 39% 감소함을

의미한다. 즉, CISO를 겸직하지 않았을 때 ISMS 인증을 받을 확률이 낮아져 다른 인증들과 반대의 결과를 보였다〈표 7〉.

즉, CISO를 겸직하지 않았을 때 정보보호 인증을 받을 확률이 증가하는 순서는 ISO27001 및 ISMS → ISMS-P → ISO27001 및 ISMS-P → ISO 27001 → ISMS 순으로 나타났으며, ISMS의 경우 자율적으로 취득하는 다른 정보보호 인증과 달리 의무로 취득해야 함에 있어서 결과 값이 달랐던 것으로 추측된다. 해당 결과들의 유의성 검정 결과는 〈표 6〉에서의 결과처럼 통계적으로 유의미한 것으로 확인되었으며, 따라서 CISO의 겸직 여부가 정보보호 인증 취득에 유의미한 인과관계를 미치는 것으로 나타났다.

〈표 7〉 CISO 겸직 여부가 정보보호 인증 종류별 취득에 미치는 영향

종속변수	독립변수	계수(B)	표준오차(S.E.)	왈드 통계량(Wald)	자유도	유의확률(p-value)	계수의 지수 Exp(B)
ISMS	겸직 여부	-0.495	0.252	3.845	1	0.050	0.610
ISMS-P		1.112	0.419	7.042	1	0.008	3.041
ISO27001		0.894	0.272	10.770	1	0.001	2.445
ISO27001 및 ISMS		1.450	0.333	18.992	1	0.000	4.264
ISO27001 및 ISMS-P		1.095	0.389	7.918	1	0.005	2.990

3.2.2 CISO 겸직에 따른 투자액 및 인력 차이 분석

기업에서 정보보호 투자액과 정보보호 인력의 확보는 정보보안을 강화하는데 가장 기본적이면서 중요한 요소이다. CISO의 겸직 여부에 따라 정보보호 투자액과 정보보호 인력규모의 차이가 있는지를 검증하기 위해 독립표본-t 검정을 실시하였다. 공시기업 660개 중 Google, 아마존 등 해외 본사에서 투자 관련 의사결정을 함에 따라 한국 지사 또는 사무소에서 매출액 및 인력 확인이 어려운 기업과 삼성전자와 같은 절대수치가 커서 평균값에 영향을 주는 데이터 17개를 제외하고 총 643개 회사에 대해 분석하였다. 정보보호 투자액과 정보보호 인력의 통계를 확인하였을 때, 겸직을 하지 않은 경우 정보보호 투자액의 평균은 3,511,398,072원이며, 정보보호 인력의 평균은 14.6명이었다. 반면에, 겸직을 한 경우, 정보보호 투자액의 평균은 1,260,696,339원이고, 정보보호 인력의 평균은 5.0명으로 두 지표 모두 겸직을 하지 않은 경우보다 매우 낮았다. 즉, CISO를 겸직하지 않았을 때가 CISO를 겸직했을 때보다 정보보호 투자액과 인력이 많은 것으로 확인되었다.

해당 독립표본-t 검정에 대한 유의성 검증 결과 t의 값이 크고 유의확률이 0.05보다 낮을수록 두 집단 간의 평균 차이가 통계적으로 유의미하다고 나타낼 수 있는데, t-값이 4.679와 5.968으로 큰 값이 나왔으며, 유의확률이 유의수준인 0.05보다 낮은 0.000으로 나왔으므로, CISO를 겸직 여부에 따라 정보보호 투자액과 정보보호 인력의 차이가 통계적으로 유의미하게 다르다고 해석된다.

즉, 독립 표본-t 검정 결과를 해석하면 CISO 겸직하지 않았을 때가 CISO를 겸직 했을 때보다 정보보호 투자액과 정보보호 인력이 더 증가했다는 결과가 통계적으로 유의미하다는 결과가 도출됐다〈표 8〉.

〈표 8〉 CISO 겸직에 따른 정보보호 투자액 및 인력 차이 평균 t-검정

평균, 표준편차 단위: 원

	겸직 여부	N	평균	표준편차	t(p)
정보보호 투자액	겸직 안함	182	3,511,398,072	6,840,369,099	4.679 (0.000)
	겸직 함	461	1,260,696,339	4,863,385,427	
정보보호 인력	겸직 안함	182	14.6	26.3	5.968 (0.000)
	겸직 함	461	5.0	14.0	

3.2.3 CISO와 겸직 CXO 비율 분석

기업에서 CISO는 어떤 CXO와 겸직을 수행하느냐에 따라 CISO의 업무에 큰 영향을 미칠 수 있다. 이에 따라 어떤 CXO와 겸직을 많이 수행하고 있는지 2022년도 정보보호 공시기업 660개를 대상으로 겸직 CXO 별 건수와 비율을 조사하였다. 이를 위해 공시 데이터 상 CISO 겸직 여부에 명확하게 CXO라고 기재한 건수만을 대상으로 하였다. 그 외 대표이사, 사장, 병원장의 경우 CEO(Chief Executive Officer, 최고책임자)로 분류하였고, 부사장, 부원장, 행정부원장, 진료부원장은 EVP(Executive Vice President, 최고부책임자)로 분류하여 다중 분석한 결과 총 41.1%인 271개의 기업에서 CXO가 CISO와 겸직을 하고 있었으며, 겸직 CXO는 총 318건으로 조사되었다〈표 9〉.

겸직 CXO 중 가장 높은 빈도는 CPO(Chief Privacy Officer, 개인정보보호책임자)가 199건(62.6%)이었고, 두 번째로 높은 빈도는 CFO(Chief Financial Officer, 재무최고책임자)로 31건(9.7%)이었다. 그 밖에, EVP 28건(8.8%), CIO(Chief Information Officer, 정보관리최고책임자) 25건(7.9%), CEO 24건(7.5%), CTO(Chief Technology Officer, 기술최고책임자) 4건(1.3%), CSO(Chief Security Officer, 보안최고책임자) 3건(0.9%)이었으며, CDO (Chief Digital Officer, 디지털최고책임자), CHO (Chief Human resource Officer, 인사최고책임자), CLO(Chief Legal Officer, 법률최고책임자) DPO(Data Protection Officer, 데이터보호책임자)는 각각 1건(0.3%)이었다〈표 10〉.

해당 결과를 살펴보면, 『정보통신망법』에서도 겸직이 허용되어 있는 CPO가 당연 압도적으로 많았고, 최고경영진인 CEO와 EVP도 겸직을 많이 하는 것으로 나타났다. 또한, 전산 업무를 수행하는 CIO도 겸직을 많이 하는 것으로 나타났으나, 의외로 업무 연관성이 낮은 CFO가 2번째로 겸직을 많이 수행하고 있었다. 이에 따라 4장에서 최고경영진(CEO, EVP)을 제외한 겸직 비율이 높은 CXO 3개를 선정하여 CISO의 업무와 연관성이 있는지 분석하였다.

〈표 9〉 겸직 CXO 비율_요약

	유효		결측		전체	
	기업 수	퍼센트	기업 수	퍼센트	기업 수	퍼센트
겸직CXO	271	41.1%	389	58.9%	660	100%

〈표 10〉 겸직 CXO 비율_상세

겸직 CXO	건수	퍼센트
CPO (Chief Privacy Officer)	199	62.6%
CFO (Chief Financial Officer)	31	9.7%
EVP (Executive Vice President)	28	8.8%
CIO (Chief Information Officer)	25	7.9%
CEO (Chief Executive Officer)	24	7.5%
CTO (Chief Technology Officer)	4	1.3%
CSO (Chief Security Officer)	3	0.9%
CDO (Chief Digital Officer)	1	0.3%
CHO (Chief Human resource Officer)	1	0.3%
CLO (Chief Legal Officer)	1	0.3%
DPO (Data Protection Officer)	1	0.3%
전체	318	100.0%

Ⅳ. 겸직 비율이 높은 CXO 업무와 역할

4.1 CISO 업무와 비교할 CXO 선정

〈표 10〉의 조사결과를 통해 겸직 비율이 높은 3개의 CXO를 선정하여 해당 CXO는 어떤 업무를 수행하는지 확인하여 CISO 업무와의 차이점을 파악하였다. 상위 3개의 CXO를 선정하면 CPO, CFO, EVP이나, 『정보통신망법』에도 겸직이 허용되어 있으며 CISO의 업무와 유사성이 있는 CPO는 선정 대상에서 제외하였고, 다른 최고책임자 직무와 겸직이 가능한 최고 경영자 위치인 CEO와 EVP 또한 선정 대상에서 제외하여 업무 비교할 CXO로 CFO, CIO, CTO를 선정하였다

4.2 CFO의 역할과 업무

CFO는 1962년 미국 컨트롤러협회(Controllers Institute of America)가 그 이름을 금융경영연구원(Financial Executives Institute, FEI)로 변경한 것이 CFO의 지위에 중요한 전환점이 되었으며, 이 무렵 CFO라는 직함이 명함과 사무실에 나타나기 시작하였다. 미국 기업에서 공식적으로 CFO 직위를 임명한 첫 번째 기업은 1966년 2월 Dan River Mills Inc.에서 Eugene Rowe를 부사장과 CFO로 겸직 임명한 것이며, 이후 CFO를 임명하는 기업들이 조금씩 생겨나기 시작하여, 2000년에 관측 시에는 80% 이상으로 증가했다. Mian(2001)은 CFO의 주요 책임이 "기업의 재무 시스템 관리"로, 일반적으로 재무 보고서 준비를 감독하고 재무 전략의 외부 커뮤니케이션을 위한 담당자 역할을 하며 자본 조달과 관련된 활동에 대한 궁극적인 책임을 지고 월스트리트의 주요 연락처 역할을 한다고 했다. 또한, CFO의 역할에는 관리/원가 회계, 재무 회계 또는 재무부와 같은 주요 재무 및 회계 기능에 대한 감독도 포함된다고 하였다. Cambridge Business English Dictionary에서는 CFO를 "회사나 조직에서 가장 중요한 재무 관리자이자 재무부서의 책임자"라고 정의했으며, Hoitash et al.(2016)은 일반적으로 CFO는 회사의 회계 및 모든 재무기능을 관리하며, CFO의 책임에는 예산, 기업 지출, 내부 통제 관리, 재무 보고 감독 및 회계 규정 준수 보장이 포함된다고 하였다.

위와 같이 CFO의 문헌들을 참조하였을 때, CFO는 기업 내 재무 전문가에게 주어지는 가장 높은 직급으로 소속 기업의 재무 상태 전반을 책임지는 것이 업무로 조사되었다. 이를 통해 CFO와 겸직 시 정보보안 예산과 관련된 이슈에 대해 보다 효율적으로 대처할 수 있으며, 보안에 대한 전략적인 방침을 수립할 수 있는 장점이 있지만, CISO와 업무 연관성이 낮기 때문에 정보보안 업무를 수행하는 데 어려움이 있을 수 있다는 단점이 있다. CFO와 CISO가 위험을 종합적으로 평가하고 관리하는 공통점과, 비용 관리와 보안 간의 균형을 효율적으로 관리하기 위해 많은 기업에서 겸직을 수행하는 것으로 판단된다.

4.3 CIO의 역할과 업무

CIO(Chief Information Officer)는 1970년대까지는 정보시스템 관리자 또는 자료처리 관리자라는 용어로 사용하였으며, IT 관리의 중요성이 부각되면서 1980년대부터 연구에서 처음 사용되었다. 1980년대에 CIO는 IT 운영에 중점을 두고 "계속 조명" 하는 기술자에서 전략적으로 중요한 이니셔티브를 주도하는 총괄 관리자로 진화했다. 1990년대에 CIO는 정기적으로 증가하여 임원으로 승진했으며 종종 CXO의 일부가 되었다. 또한 점점 더 많은 CIO가 CEO에게 직접 보고하기 시작하고 IT 부서 외부의 상호 작용에 더 많은 시간을 할애함에 따라 비즈니

스가 광범위 해졌다. 조직 내에서 IT의 중요성이 빠르게 증가하면서 CIO 역할은 기업의 전략에 초점을 맞추면서 IT를 계속 운영하고 IT 투자에 대한 높은 수익을 달성하는 비즈니스 비전가로 전환되었다. 이후 CIO의 가치와 효과, 그리고 조직성과에 대한 역할의 영향에 대한 논쟁이 더욱 주목을 받았으며, 역할 효율성을 높이기 위해 Peppard et al.(2011)는 경쟁 우위를 위한 IT의 중요성과 조직의 IT 리더십 기능의 성숙도를 기반으로 5가지 고유한 역할 유형 중에서 적절한 CIO를 결정할 것을 제안하였다.

위와 같이 CIO의 문헌들을 참조하였을 때, CIO는 정보관리책임자로 조직의 IT 경영과 전략적인 관점에서 IT 및 정보 시스템을 총괄 관리 책임을 지는 것이 업무로 조사되었다. 이를 통해 CIO 겸직 시 IT 업무가 주 업무이기 때문에 CISO 업무에 대한 이해도가 높고 서로 상호 보완적인 역할을 수행할 수 있는 장점이 있으나, CIO의 업무가 주로 IT 관리, IT 지원 등 효율성과 편의성에 중점을 두다 보니 정보보안의 업무와 충돌될 수 있다는 단점이 있다. CISO라는 직책이 생기기 이전에 CISO의 업무를 CIO가 수행하였고, IT관련 업무를 공통적으로 수행하기 때문에 기업에서 예산 및 인력 부족 등의 사유로 아직까지 CIO가 CISO의 업무를 많이 수행하고 있는 것으로 판단된다.

4.4 CTO의 역할과 업무

Delmar(2003)에 의하면, CTO(Chief Technology Officer)라는 직함이 1980년대에 처음 등장하였으며, 상세하게 논의된 논문은 Adler & Ferdows(1990)의 것으로, CTO가 다양한 비즈니스에 걸쳐 있어 오늘날 많은 조직에서 기술에 대한 특정 책임을 가진 관리자가 있어야 한다고 하였다. Medcof(2007)는 2007년 CTO 역할을 최고 기술 책임자(CTO)는 기업의 기술을 책임지는 최고 경영진이며 이상적으로는 회사 전략을 수립하고 기술 고려 사항이 해당 전략에 최적으로 통합되도록 하는 데 중요한 역할을 한다고 정의했으며, 2008년에는 CTO에 대한 정의를 일반적으로 회사에서 가장 높은 순위의 기술 관리자이며 일부 조직에서는 해당 직위를 기술 부사장이라고 확장했다. Smith(2007)는 CTO는 기업의 수익과 미래 경쟁 우위에 대한 기여도에 따라 혁신, 연구 및 실험을 측정하는 사업가라 하였으며, 현대의 CTO 직위는 기술적 능력을 전략적 비즈니스 결정으로 전환할 수 있는 기술자 또는 과학자를 요구한다고 하였다. Hartley(2011)는 CTO의 연구를 광범위하게 분석하여 요약하였는데 CTO 역할의 진화와 관련이 있는 두 가지 핵심 사항, 즉 기술 관리를 위한 환경 변화와 CTO의 특정 책임에 대한 연구를 요약하였으며, 최근 수십 년 동안 개발 중인 기술의 범위와 기술이 등장하는 속도가 증가하여 CTO의 책임이 확대되고 있다고 하였고, Robb(1994)는 CTO의 역할이 기술에 대한 투자의 장기적인 성장을 보장하기 위해 기술 개발 예산을 방어하는 것이라고 주장하였다.

위와 같이 CTO의 문헌들을 참조하였을 때, CTO는 기업에서 효과적으로 기술을 획득, 관리 및 활용하기 위한 모든 경영지원 활동을 총괄책임을 지는 것이 업무로 조사되었다. 이를 통해 CTO 겸직 시에도 CIO와 동일하게 CISO의 업무 이해도가 높다는 장점이 있으나 개발에 중점을 두다 보니 개발 업무와 정보보안 업무의 상호 간 견제가 필요한 모순적 의사결정을 해야 하는 상황이 올 수 있다는 단점이 존재한다. CIO와 마찬가지로 CTO도 CISO와 IT업무를 공통적으로 수행하기 때문에 기업에서 예산 및 인력 부족 등의 사유로 아직까지 CTO가 CISO의 업무를 많이 수행하고 있는 것으로 판단된다.

겸직 비율이 높은 3개의 CXO를 선정하여 해당 CXO는 어떤 업무를 수행하는지 확인한 결과 CFO는 재무 총괄 책임 업무가 주 업무이며, CIO는 IT 운영 총괄 책임 업무, CTO는 기술 관리 총괄 책임 업무

를 주 업무로 수행하여 각 CXO의 업무가 명확하게 구분되어 있음을 확인하였다. 위 3개의 CXO가 겸직을 수행했을 때의 장·단점 이외에, CXO들이 겸직을 수행하면서 생기는 공통적인 장·단점으로는 인력 비용을 절감할 수 있고, 두 역할을 함께 수행함으로써, 시너지를 창출할 수 있다는 장점이 있지만, 두 업무 영역이 겹칠 경우 혼란이 생길 수 있으며, 집중력 분산 및 본 업무에 비중을 두어 정보보안의 업무가 우선순위에 밀려 CISO의 업무가 소홀해질 수 있는 단점도 있다〈표 11〉.

〈표 11〉 CISO 겸직 시 CXO 별 장·단점

겸직 CXO	장점	단점
CFO	· 예산 확보 수월 · 전략적 방침 수립	· 전문성 저하
CIO CTO	· 전문성 보유로 인한 효율적인 업무 수행	· 역할 충돌
공통	· 인력 비용 절감 · 시너지 효과 발휘	· 업무 혼란 · 업무 우선순위 고려

Ⅴ. 결론 및 향후 연구

5.1 연구 결과 및 시사점

정보보호 공시 데이터를 활용하여 다양한 측면에서 심층 분석을 실시한 결과는 다음과 같다.

첫 번째로, 대다수의 기업이 정보보호 인증(ISMS-P, ISO27001, ISO27001 및 ISMS, ISO27001 및 ISMS-P)이 CISO를 겸직하지 않았을 때 겸직을 했을 때보다 인증 취득의 경우가 높은 것을 확인할 수 있었지만, ISMS의 경우에는 반대로 겸직을 했을 때 인증 취득할 확률이 높아지는 결과를 보였다. 자율적으로 취득하는 다른 정보보호 인증과 달리 의무로 취득해야 함에 있어서 결과가 달랐던 것으로 추측된다.

두 번째로, CISO의 겸직 여부에 따라 정보보호 투자액, 정보보호 인력의 차이가 있음을 확인하였으며, 겸직을 하지 않았을 때 정보보호 투자액, 정보보호 인력이 보다 많은 것을 확인할 수 있었다. 이러한 결과는 기업의 정보보호를 강화하기 위해서는 충분한 정보보호 투자 및 정보보호 인력 확보가 필요하고 선행과정으로 CISO를 겸직하지 않도록 지향해야 한다는 시사점을 제공한다.

마지막으로, 겸직 비율이 높은 3개의 CXO를 선정하여 해당 CXO는 어떤 업무를 수행하는지 확인한 결과 CFO는 재무 총괄 책임 업무가 주 업무이며, CIO는 IT 운영 총괄 책임 업무, CTO는 기술 관리 총괄 책임 업무를 주 업무로 수행하여 각 CXO의 업무가 명확하게 구분되어 있음을 확인하였다. CXO들이 겸직을 수행하면서 생기는 공통적인 장·단점으로는 인력 비용을 절감할 수 있고, 두 역할을 함께 수행함으로써, 시너지를 창출할 수 있다는 장점이 있지만, 두 업무 영역이 겹칠 경우 혼란이 생길 수 있으며, 집중력 분산 및 본 업무에 비중을 두어 정보보안의 업무가 우선순위에 밀려 CISO의 업무가 소홀해질 수 있는 단점도 있다

하지만 대부분의 기업이 예산, 내부 조직 구조 등으로 인해 의도치 않게 CISO의 겸직을 수행하는 경우가 많다. 이와 같이 부득이하게 겸직을 수행하는 경우 『정보통신망법』 적용 대상이 아니더라도 〈표 2〉에 해당되는 CISO 업무 4가지는 정보보안 업무의 최소한의 업무로 수행하여야 할 것이다. 본 연구는 정보보호 공시기업의 정보보호에 대한 심층 분석을 통해 CISO의 역할과 정보보호 인증 취득, 그리고 CXO의 겸직 여부와 정보보호 투자액 및 인력의 관계 등을 분석하여 다음과 같은 시사점을 제공한다.

첫째, CISO 겸직이 정보보호 인증 취득 종류별로 미치는 영향. 둘째, CISO의 겸직 여부에 따른 정보보호 투자액 및 정보보호 인력 평균의 차이. 셋째,

CFO, CIO, CTO의 역할과 업무, CXO 별 겸직 시장·단점 등을 밝혔다. 이러한 결과를 종합해보면, 기업마다 예산 및 인력 부족 등 부득이한 사유로 CISO를 겸직하는 경우가 많으나, 정보보안 사고가 발생하면 더 큰 예산과 인력이 낭비 될 수 있다. 정보보안을 강화하기 위해 CISO의 겸직을 가급적이면 제한하여 정보보호 인증을 취득하고, 정보보호 예산과 인력을 확보하여야 한다. 또한 부득이하게 겸직을 수행하더라도 정보보호 업무의 우선순위와 집중력 분산 문제를 고려해야 한다는 것이 중요한 시사점이다. 겸직 시 인력 비용 절감과 시너지 창출 등의 장점도 있지만, 정보보호 업무의 소홀함 등으로 인해 더 큰 문제가 발생할 수 있으므로, 기업은 적절한 역할 분담과 역할 및 책임의 명확한 정의 등을 고려하여 정보보호를 강화할 필요가 있다.

5.2 연구의 한계와 향후 연구 방향

본 논문은 다음과 같은 한계점을 가지고 있다. 첫째, 겸직 여부에 따라 실제 CISO의 업무 수행성과에 차이가 있는지를 확인하지 못했다. 둘째, CISO를 겸직하지 않았을 때 ISMS 인증을 취득할 확률이 낮아지는 사유를 구체적으로 확인하지 못했다. 셋째, 정보보호 공시 자료만을 기반으로 하여 데이터 수집량이 부족하다. 넷째, 겸직 시 수행해야 할 최소한의 정보보안 업무가 구체적으로 정의되지 않았다. 다섯번째, CISO의 겸직 시기를 확인할 수 없었다. CISO와 겸직한 시기를 알 수 있다면, 정보보호 인증을 취득한 시기와 비교하여 겸직으로 인한 변화 여부를 확인 가능했을 것이다. 마지막으로, 정보보호 공시 자료만을 활용하다 보니 CISO 겸직 전후를 비교할 수 있는 통제 변수 확보가 불가능하였다. 향후 연구 시 인터뷰 및 설문 조사 등 조사연구를 통해 데이터 수집을 확대하고, 공시 대상 기업의 규모, 정보보안 사고 건수, 피해액 등 통제변수 데이터를 확보하여 CISO 겸직 여부로 인한 성과 측정을 좀 더 구체적으로 정의할 것이며, 겸직 시 수행해야 할 최소한의 정보보안 업무에 대해 조사하여 수행 업무를 보다 명확하게 정의할 것이다. 이러한 연구를 통해 이 논문의 한계를 극복하고 보다 심도 있는 연구를 수행할 수 있을 것으로 기대한다.

REFERENCES

Adler, P. S. and Ferdows, K.(1990), "The chief technology officer," *California Management Review*, 32(3), 55-62.

Aguas, T., Kark, K. and François, M.(2016), "The New CISO," *Deloitte Review*, 19, 73-89.

Applegate, L. M. and Elam, J. J.(1992), "New information systems leaders: A changing role in a changing world," *MIS Quarterly*, 16(4), 469-490.

Ashenden, D. and Sasse, A. (2013), "CISOs and organisational culture: Their own worst enemy?," *Computers & Security*, 39(B), 396-405.

Baskerville, R. and Dhillon, G.(2008), "Information Systems Security Strategy: A Process View," In Straub, D., Goodman, S. and Baskerville, R. (Eds.), Information Security: Policy, Processes, and Practices (pp.15-45). Armonk: M E Sharpe.

Benjamin, R. I., Dickinson Jr, C. and Rockart, J. F.(1985), "Changing role of the corporate information systems officer," *MIS Quarterly*, 9(3), 177-188.

Bremer, D. (2010), "The effect of stakeholder influence on CFO and CEO turnover in German Corporate Governance," (Dissertation). Otto Beisheim School of Management.

Cambridge Business English Dictionary(2021), "Chief Financial Officer definition."

Chun, M. and Mooney, J.(2009), "CIO roles and responsibilities: Twenty-five years of evolution and change," *Information & Management*, 46(6), 323-334.

Delmar, D. R.(2003), "The rise of the CSO (Organization Design)," *Journal of Business Strategy*, 24 (2), 8-11.

Eisenhardt, K. M.(1989), "Agency theory: An assessment and review," *Academy of Management Review*, 14(1), 57-74.

Fisher, R. A.(1925), "Theory of statistical estimation," *Proceedings of the Cambridge Philosophical Society*, 22(5), 700-725.

Grover, V., Jeong, S. R., Kettinger, W. J. and Lee, C. C.(1993), "The chief information officer: A study of managerial roles," *Journal of Management Information Systems*, 10(2), 107-130.

Hardy, C. (1996), "Understanding power: bringing about strategic change," *British Journal of Management*, 7(S1), S3-S16.

Hartley, S. (2011), "The effectiveness of the chief technology officer," *Research-Technology Management*, 54(3), 28-35.

Hiebl, M. R. W.(2013), "Bean counter or strategist? Differences in the role of the CFO in family and non-family businesses," *Journal of Family Business Strategy*, 4(2), 147-161.

Hoitash, R., Hoitash, U. and Kurt, A. C.(2016), "Do accountants make better chief financial officers?," *Journal of Accounting and Economics*, 61(2-3), 414-432.

Hosmer Jr, D. W., Lemeshow, S. and Sturdivant, R. X.(2013), *Applied Logistic Regression*, John Wiley & Sons.

Information Security Disclosure Portal(2022), *Analysis Report on the 2022 Information Security Disclosure Status*. [printed in Korean]

Information Security Disclosure Portal(2023), *Guidelines for Information Security Disclosure*. [printed in Korean]

Karaian, J.(February 20, 2014), "The chief financial officer: What CFOs do, the influence they have, and why it matters," The Economist Newspaper.

Karanja, E. and Rosso, M. A.(2017), "The chief information security officer: An exploratory study," *Journal of International Technology and Information Management*, 26(2), 23-47.

Kayworth, T. and Whitten, D.(2010), "Effective information security requires a balance of social and technology factors," *MIS Quarterly Executive*, 9(3), Article 5.

Kim, Jisoo, Kim, Jongbae and Shin, Yongtae(2012), "A study on the impact of Chief Information Security Officer (CISO)'s role perception on information security performance within the organization," *Management Consulting Research*, 12(4), 21-34. [printed in Korean].

Kotulic, A. G. and Clark, J. G.(2004), "Why there aren't more information security research studies," *Information & Management*, 41(5), 597-607.

Medcof, J. W.(2007), "CTO power," *Research-Technology Management*, 50(4), 23-31.

Medcof, J. W.(2008), "The organizational influence of the chief technology officer," *R&D Management*, 38(4), 406-420.

Mian, S.(2001), "On the choice and replacement of chief financial officers," *Journal of Financial Economics*, 60(1), 143-175.

Ministry of Science, ICT and Future Planning & Korea Information Security Industry Association (2022), *2021 Information Security Status Survey Report*. [printed in Korean]

Peppard, J.(2010), "Unlocking the performance of the chief information officer (CIO)," *California Management Review*, 52(4), 73-99.

Peppard, J., Edwards, C. and Lambert, R. (2011), "Clarifying the Ambiguous Role of the CIO," *MIS Quarterly Executive*, 10(1), 31-44.

Preston, D. S., Chen, D. and Leidner, D. E.(2008), "Examining the antecedents and consequences of CIO strategic decision-making authority: An empirical study," *Decision Sciences*, 39 (4), 605-642.

Robb, W. L.(1994), "Selling technology to your CEO," *Research-Technology Management*, 37(5), 43-45.

Rockart, J. F., Ball, L. and Bullen, C. V.(1982), "Future role of the information systems executive," *MIS Quarterly*, 6(4), 1-14.

Ross, J. W. and Feeny, D. F.(2000), "The evolving role of the CIO," *Pinnaflex Educational Resources*, 308, 385-402.

Smith, R.(2007), "What CTOs do," *Research-Technology Management*, 50(4), 18-22.

Smith, R. D.(2003), "The chief technology officer: Strategic responsibilities and relationships," *Research-Technology Management*, 46(4), 28-36.

Stephens, C. S., Ledbetter, W. N., Mitra, A. and Ford, F. N.(1992), "Executive or functional manager? The nature of the CIO's job," *MIS Quarterly*, 16(4), 449-467.

Synnot, W. R. and Gruber, W. H.(1981), *Information Resource Management*, John Wiley & Sons, New York.

Weill, P. D. and Woerner, S.(2013), "The future of the CIO in a digital economy," *MIS Quarterly Executive*, 12(2), 65-75.

Zorn, D. M.(2004), "Here a chief, there a chief: The rise of the CFO in the American firm," *American Sociological Review*, 69(3), 345-364.

국내참고문헌

고규만(2010), "정보보호관리체계(ISMS) 인증의 경제적 효과 분석," **인터넷 이슈**, 2, 23-47.

과학기술정보통신부, 한국정보보호산업협회(2022), 2021년 정보보호 실태조사 보고서.

김지수, 김종배, 신용태(2012), "조직내 정보보호최고책임자(CISO)의 역할인식이 정보보호성과에 미치는 영향에 관한 연구," **경영컨설팅연구**, 12(4), 21-34.

배영식(2012), "정보보호관리체계 〔ISMS〕 인증이 조직성과에 미치는 영향에 관한 연구," **한국산학기술학회 논문지**, 13(9), 4224-4233.

정보보호 공시 종합 포털(2022), 2022 정보보호 공시 현황 분석보고서.

정보보호 공시 종합 포털, 정보보호 공시 가이드라인, 2023.

『정보보호산업의 진흥에 관한 법률』(2023.10.19. 시행), 국가법령정보센터.

『정보통신망 이용촉진 및 정보보호 등에 관한 법률』(2023.7.4. 시행), 국가법령정보센터.

『개인정보 보호법』(2023.9.15. 시행), 국가법령정보센터.

『전자금융거래법』(2020.12.10. 시행), 국가법령정보센터.

Dual Positions of Chief Information Security Officer, and Performance of Information Security: Focusing on Information Security Disclosure Data

Don Su Choi* · Tae-Sung Kim**

Abstract

In February 2012, the revised "Information and Communication Network Act" introduced the executive-level appointment system for the Chief Information Security Officer (CISO). However, even after a decade, many public institutions and private companies still fail to recognize the significance of CISO or have the Chief X Officers (CXOs) take on CISO responsibilities concurrently, resulting in inadequate performance of CISO duties.

This study aims to investigate the impact of CISO's dual role on obtaining information security certifications by analyzing data from companies that have submitted information security disclosure documents. Additionally, it seeks to examine whether there are differences in information security investment and workforce depending on the dual role of CISO. Furthermore, the study explores CXOs with high rates of dual roles to distinguish their responsibilities and identify any issues that may arise from such dual appointments.

Results of this study are expected to help companies strengthen their information security by considering appropriate role allocation, clear definition of roles and responsibilities, and address potential problems associated with dual appointments.

Key Words: CISO, Dual Position, Information Security Performance, Information Security Disclosure, CXO

* Master student, Department of Convergence Security, Chungbuk National University, First Author
** Professor, Department of Management Information Systems, and Department of Convergence Security, Chungbuk National University, Corresponding Author