# 정보보호 최고책임자(CISO)의 법적 지위 제안

윤승용, 원유재
충남대학교 컴퓨터공학과
yoon.seungyong@o.cnu.ac.kr, yjwon@cnu.ac.kr

# Suggestions for Legal Status of Chief Information Security Officer (CISO)

SeungYong Yoon, Yoojae Won
Dept. of Computer Science Engineering, Chungnam National University

요 약

지능정보사회의 발전에 따라 사이버 공격은 업종과 규모를 가리지 않고 모든 기업을 대상으로 이뤄지고 있다. 이러한 현실을 반영하여 최근 정보통신망법은 모든 정보통신서비스 제공자에게 특정 지위의 정보보호 최고책임자(CISO)를 지정하도록 개정되어 시행될 예정이다. 그러나 정보통신망법령은 업종별 정보화 특성을 고려하지 아니하고, 매출액·자산총액 기준으로만 정보보호 최고책임자의 지위를 차등화하고 있으며, 차등화된 지위는 임원·비임원 여부로만 규정되어 있어 현장에서 실효성이 발휘되기 곤란하다는 문제가 있다. 본 논문은 정보보호 거버넌스 관점에서 지위를 차등화하고 업종별 특성과 종업원 수 기준에 따른 정보보호 최고책임자의 법적 지위 요건을 제시하고자 한다.

## 1. 서론

최근 사이버 공격은 개인정보를 다루는 인터넷 기업뿐만 아니라 미국 최대 송유관 업체 콜로니얼 파이프라인 랜섬웨어 해킹 사태, 국내 위즈베라 베라포트 공급망 공격 등에서 알 수 있듯이 업종과 규모를 가리지 않고 모든 기업을 대상으로 이뤄지고 있다. 우리나라는 사이버 공격으로 인한 각종 침해사고로부터 이용자를 보호하기 위해 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 “정보통신망법”)을 통해 정보통신서비스 제공자[1]에게 정보보호 최고책임자(CISO; Chief Information Security Officer)를 지정·신고하도록 의무를 부과하고 있다.

정보보호 최고책임자 제도의 실효성을 강화한 정보통신망법이 2021년 6월 8일에 개정되어 2021년 12월 9일에 시행될 예정이며, 과학기술정보통신부는 세부 기준을 구체화한 정보통신망법 시행령 일부개정령(안)을 2021년 8월 3일부터 입법예고하고 있다. 입법예고안은 정보통신서비스 제공자는 매출액·자산총액에 따라 정보보호 최고책임자를 이사 또는 사업주 직속 부서장(비임원)으로 지정하거나 사업주를 정보보호 최고책임자로 간주하도록 규정하고 있다.

임원이나 관리자를 두어야 하는 법적 의무가 실효성을 확보하려면 기업의 조직 개편이 동반되어야 하므로 정보보호 최고책임자의 지위를 규정하는 법적 의무는 개정 규정과 같은 매출액·자산총액 등의 통화기반이 아닌 종사자 수를 기준으로 규정되어야 한다. 최근 사이버 공격의 행태 상 정보통신망을 이용하는 모든 기업은 업종을 불문하고 정보보호 최고책임자를 둘 필요가 있으나 그 지위를 규정하는 법적 의무는 업종별 특성과 침해사고 발생 시 국민에게 미치는 영향을 고려하여 기업이 적절한 정보보호 조직을 구성할 수 있도록 부과되어야 한다. 정보보호 최고책임자 제도 도입 연구[2]는 기업 규모와 업종에 따라 정보보호 최고책임자의 지위를 차등화하는 것이 바람직하다고 언급하고 있다. 한편, 전사 조직에 행사되는 정보보호 영향력은 정보보호 최고책임자의 정보보호 거버넌스 상 역할에 따라 달라지므로 정보보호 최고책임자의 지위는 현행 규정과 같은 임원·비임원 여부가 아닌 정보보호 거버넌스에서의 역할별로 차등화되어야 한다. 본 논문은 정보보호 거버넌스의 역할별로 지위를 분류하고, 업종별 국가에 미치는 영향력과 정보화 정도, 종업원 수에 따른 정보보호 최고책임자의 법적 지위 기준을 제안한다.

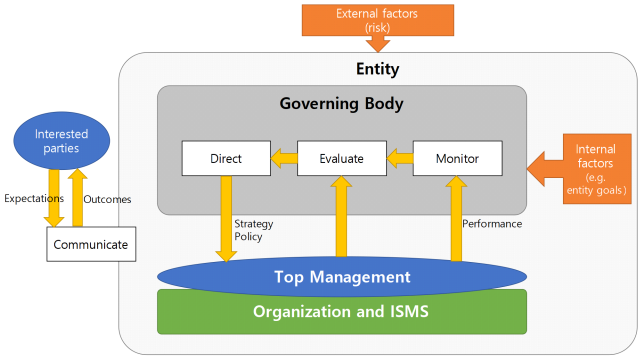
본 논문의 구성은 다음과 같다. 2장에서 정보보호 거버넌스와 정보보호 최고책임자의 역할을 소개하고, 3장에서 정보통신망법 상 정보보호 최고책임자 제도를 설명한다. 4장에서 정보보호 최고책임자의 법적 지위 요건을 제안하고, 5장에서 제안한 지위 요건의 적용 결과를 분석하며, 6장에서 마무리한다.

1) 정보통신서비스 제공자는 전기통신사업자(기간통신사업자, 부가통신사업자)와 영리를 목적으로 정보통신서비스를 제공하거나 매개하는 자를 말하며, 업종과 상관없이 홈페이지를 운영하거나 SNS, 오픈마켓 등을 이용하여 서비스를 제공하는 모든 상법 상 상인 및 회사가 해당한다[1].

## 2. 정보보호 거버넌스와 정보보호 최고책임자

### 2.1. 정보보호 거버넌스

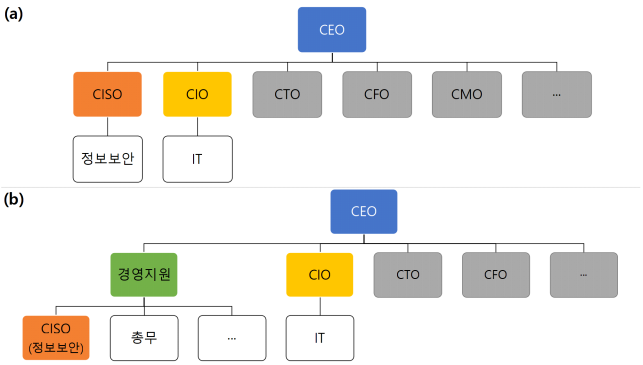
정보보호 거버넌스는 기업 보안 프로그램의 전략적 방향을 제시하고, 목표의 달성 여부를 확인하며, 위험을 적절하게 관리하고, 조직의 자산을 책임 있게 활용하며, 이를 위한 체계가 적절하게 작동하고 있는지 모니터링하기 위해 기업 경영진에게 제공하는 메커니즘, 프로세스 및 관계를 의미한다. 정보보호 거버넌스 국제표준인 ISO/IEC 27014:2020[3]은 그림 1과 같이 정보보호 거버넌스 모델을 제시하고 있다. 엔티티(entity)[2]에 속한 이사회(governing body)[3]는 "평가(evaluate)", "지시(direct)", "관찰(monitor)", "소통(communicate)" 프로세스를 수행한다. 최고경영진(top management)[4]은 조직(organization)[5]에 권한을 위임하고 자원을 제공한다. 이사회는 보안 목표 달성의 현 수준과 향후 계획을 '평가'하고, 최고경영진에게 엔티티의 목표와 전략, 정책을 '지시'하며, 전략적 목표 달성을 평가하기 위해 최고경영진의 성과를 '관찰'하고, 이해관계인(interested party)들과 기대와 성과에 대해 '소통'한다. 정보보호 거버넌스에 대한 책임이 있는 주체는 이사회이며, 일반적으로 정보보호 최고책임자는 최고경영진으로서 이사회가 경영방침에 따른 기업의 보안 프로그램을 구축·운영하는 과정 전반을 관리·감독할 수 있도록 보조하는 역할을 수행한다[4, 5].




(그림 1) 정보보호 거버넌스 모델

### 2.2. 정보보호 조직체계

정보보호 조직체계를 구성하는 방식은 기업의 사업방향과 규모에 따라 상이하고, 조직체계에 따라 정보보호 최고책임자(CISO)의 정보보호 거버넌스 내에서의 역할 또한 달라진다[6]. 그림 2는 전사 조직에서 CISO와 정보보호 전담 조직의 구성 방식을 보여준다.




(그림 2) 정보보호 전담 조직의 구성

그림 2 (a)는 CISO를 CEO 직속으로 구성하는 것을 나타낸다. CISO의 권한에 따라 CISO가 이사회의 일부로 포함되었거나, CISO가 최고경영진인 경우로 볼 수 있다. 전자의 경우 CISO가 이사회로서 직접 경영 목표에 맞춰 전사에 정보보호에 대한 영향력을 행사할 수 있고, 후자의 경우 CISO가 최고경영진으로서 이사회(CEO)와의 직접적인 소통을 통해 전사에 정보보호 영향력을 높일 수 있다. 이러한 구성에서는 IT 및 비IT 보안을 모두 전담 가능한 전문성 있는 임원급 보안책임자와 역량이 높은 보안 조직이 필요하다. 정보보호가 전사 비즈니스에 큰 영향을 미치고 역량 높은 전담 정보보호 조직을 갖출 수 있는 규모의 기업에서 이와 같은 조직을 구성한다.

그림 2 (b)는 CISO를 경영지원 소속으로 구성하는 것을 나타낸다. 정보보호 거버넌스 측면에서 CISO는 ISMS를 운영하고 최고경영진인 경영지원장을 보좌한다. 경영지원장은 전사 내부통제 업무의 일환으로 정보보호 업무를 수행하며, CISO는 경영지원장과 이사회의 의사결정을 지원한다. 기업의 규모가 작거나 정보보호가 전사 비즈니스에 미치는 영향이 작은 기업에서 이와 같은 조직을 구성한다.

### 2.3. 정보보호 최고책임자

정보보호 최고책임자는 기업의 정보보호 거버넌스 유지·관리를 총괄한다. 정보보호 최고책임자는 정보보호 전담 조직의 총괄 책임자임과 동시에 모든 전사 조직과 정보보호 관련 업무를 협력·중재한다. 또한 기업의 사업방향과 정보보호 전략을 일치시키고, 이해관계자 및 유관기관과의 정보보호 관련 의사소통을 책임지며, 경영진의 일원으로서 타 부서 경영진의 정보보호 위험에 관한 의사 결정을 지원한다.

2) 조직(organization)과 그 밖의 단체를 말하는 것으로 기업그룹, 단일 기업, 비영리단체 등이 될 수 있다.
3) 엔티티의 성과·규율에 대한 책임이 있는 사람들을 의미한다.
4) 최상위 수준에서 조직을 지시하고 통제하는 사람들을 의미하는 것으로, 조직 크기에 따라서는 이사회와 같을 수 있다.
5) ISMS를 관리·운영하는 엔티티의 부분 또는 전체를 의미한다.

## 3. 정보통신망법[6] 상 정보보호 최고책임자 제도

### 3.1. 정보보호 최고책임자의 법적 정의와 지위

정보보호 최고책임자 제도는 정보통신망법 제45조의3에 규정되어 있다. 제45조의3제1항 본문은 “정보통신서비스 제공자는 정보통신시스템 등에 대한 보안 및 정보의 안전한 관리를 위하여 대통령령으로 정하는 기준에 해당하는 임직원을 정보보호 최고책임자로 지정하고 과학기술정보통신부장관에게 신고하여야 한다”고 규정하고 있으며, 정보통신망법 시행령 일부개정령(안)[7]은 표 1과 같이 정보보호 최고책임자의 지위를 규정하고 있다. 「중소기업기본법」은 중소기업을 매출액 기준으로 분류하므로 정보통신망법은 통화기반 기준으로 정보보호 최고책임자의 지위를 차등화하고 있는 것으로 볼 수 있다.

<표 1> 정보보호 최고책임자의 법적 지위

| 대상 | 지위 |
|---|---|
| - 자본금 1억원 이하<br>- 소기업<br>- 중기업(정보통신 무관) | - 사업주 또는 대표이사 |
| - 중기업<br>· 전기통신사업자<br>· ISMS 인증의무 대상자<br>· 개인정보처리자<br>· 통신판매업자<br>- 중견기업, 대기업 | - 사업주 또는 대표이사<br>- 이사(미등기 임원 포함)<br>- 사업주로부터 직접 지시받는 정보보호 부서장 |
| - 자산총액 5조원 이상 기업<br>- 자산총액 5천억원 이상 ISMS 인증의무 대상자 | - 이사(미등기 임원 포함) |

### 3.2. 정보보호 최고책임자의 법적 업무

정보보호 최고책임자의 업무는 표 2와 같이 정보통신망법 제45조의3제4항에서 규정되고 있다. 정보보호 최고책임자의 업무는 정보보호 거버넌스 상 최고경영진이 수행해야 하는 업무로 구성되어 있다.

<표 2> 정보보호 최고책임자의 업무 (법 제45조의3제4항)

| | |
|---|---|
| **총괄 업무** | - 정보보호 계획의 수립·시행 및 개선<br>- 정보보호 실태와 관행의 정기적인 감사 및 개선<br>- 정보보호 위험의 식별 평가 및 정보보호 대책 마련<br>- 정보보호 교육과 모의 훈련 계획의 수립 및 시행 |
| **겸직 가능 업무** | - 정보보호산업법에 따른 정보보호 공시에 관한 업무<br>- 정보통신기반 보호법에 따른 정보보호책임자의 업무<br>- 전자금융거래법에 따른 정보보호최고책임자의 업무<br>- 개인정보 보호법에 따른 개인정보 보호책임자의 업무<br>- 그 밖에 이 법 또는 관계 법령에 따라 정보보호를 위하여 필요한 조치의 이행 |

## 4. 정보보호 최고책임자의 지위 요건 제안

### 4.1. 정보통신서비스 제공자의 분류

정보통신망법은 산업별로 국민에게 미치는 영향도를 고려하여 정보통신서비스 제공자가 적절한 정보보호 최고책임자를 지정할 수 있도록 의무를 부과해야 한다. 한편, 정보보호 거버넌스 측면에서는 기업의 사업방향과 부합하는 정보보호 조직이 구성되어야 하므로 기업의 정보통신망 의존도가 고려될 필요가 있다. 그리고 기업이 적절한 규모의 조직을 구성할 수 있도록 종업원 수를 고려해야 한다.

표 3은 정보통신서비스 제공자가 국민에게 미치는 영향도를 상·중·하로 분류한 결과다. 정보통신서비스 제공자의 업종 분류는 ‘제10차 개정 한국표준산업분류’를 따랐다. 「정보통신기반 보호법」 제2조제1호에 따른 정보통신기반시설에 해당하는 산업은 영향도 ‘상’을 부여하고, 「국토의 계획 및 이용에 관한 법률」 제2조제6호에 따른 기반시설에 해당하는 산업은 영향도 ‘중’을 부여하였다. ‘2020 정보화통계집’[7]에서 전사적 자원 관리(ERP) 활용 비율이 60%[8] 이상인 산업은 정보통신망 의존성이 높다고 보고, 자신의 영향도보다 한 단계 높은 영향도를 부과하였다.

<표 3> 정보통신서비스 제공자의 영향도

| 표준산업분류 | 정보통신 기반시설 | 기반시설 | 정보통신망 의존도 | 영향도 |
|---|---|---|---|---|
| C. 제조업 | | | O | 중 |
| D. 전기, 가스, 증기 및 공기 조절 공급업 | O | O | | 상 |
| E. 수도, 하수 및 폐기물 처리, 원료 재생업 | | O | | 중 |
| G. 도매 및 소매업 | | | O | 중 |
| H. 운수 및 창고업 | O | O | | 상 |
| J. 정보통신업 | O | O | O | 상 |
| K. 금융 및 보험업 | O | | O | 상 |
| L. 부동산업 | | | O | 중 |
| O. 공공 행정, 국방 및 사회보장 행정 | O | O | O | 상 |
| P. 교육 서비스업 | | O | | 중 |
| Q. 보건업 및 사회복지 서비스업 | | O | O | 상 |
| R. 예술, 스포츠 및 여가관련 서비스업 | | O | | 중 |

※ A. 농업, 임업 및 어업, B. 광업, F. 건설업, I. 숙박 및 음식점업, M. 전문, 과학 및 기술 서비스업, N. 사업시설 관리, 사업 지원 및 임대 서비스업, S. 협회 및 단체, 수리 및 기타 개인 서비스업은 영향도 ‘하’에 해당

### 4.2. 정보보호 최고책임자의 지위 요건

정보보호 최고책임자의 지위는 이사(상법에 따른 사내이사 또는 집행임원)[9], 임원급(상법 제401조의2 제1항 각 호에 해당하는 자)[10], 부서장(이사 또는 임원급으로부터 직접 지시를 받는 정보보호 관련 업무를 총괄하는 부서의 장)[11]으로 구분하고, 정보보호 거버넌스를 구축하기 곤란한 기업은 대표자(사업주 또는 상법에 따른 대표이사 또는 대표집행임원)를 정보보호 최고책임자로 간주하였다.

앞 절에서 분류한 정보통신서비스 제공자의 영향

6) 시행 2021. 12. 9. 법률 제18201호, 2021. 6. 8., 일부개정 기준
7) 과학기술정보통신부공고 제2021-711호, 2021. 8. 3. 기준
8) 전체 기업체의 전사적 자원 관리(ERP) 활용비율은 61.5%이다.
9) 법인등기된 임원을 의미하며, 법인에 대한 책임이 있으므로 정보보호 거버넌스에서 이사회로 볼 수 있다.
10) 법인등기되지 아니한 임원을 의미하며, 정보보호 거버넌스에서 최고경영진으로 볼 수 있다
11) 규모가 큰 기업에서는 부문장·센터장, 규모가 작은 기업에서는 부장 등 기업에서 가장 큰 단위 부서의 장을 의미하며, 정보보호 거버넌스에서 조직의 장으로 볼 수 있다.

도와 기업의 종업원수[12]를 기준으로 표 4와 같이 정보보호 최고책임자의 지위를 차등화하였다. 「전자금융감독규정」[13]을 참고하여 정보보호 인력 규모를 가정하였다. 종업원수가 50명 미만인 기업은 정보보호 전담 조직 구성이 곤란하므로 영향도와 무관하게 대표자를 정보보호 최고책임자로 간주하였다. 영향도 '하', 종업원수 50~249명인 기업에서의 지위를 대표자로 두고 영향도 또는 종업원수 단계가 올라갈 때마다 부서장-임원급-이사 순으로 차등화하였다.

<표 4> 정보보호 최고책임자의 지위요건

| 영향도 \ 종업원수 | ~49 | 50~249 | 250~999 | 1000~ |
|---|---|---|---|---|
| 하 | 대표자 | 대표자 | 부서장 | 임원급 |
| 중 | 대표자 | 부서장 | 임원급 | 이사 |
| 상 | 대표자 | 임원급 | 이사 | 이사 |

## 5. 정보보호 최고책임자의 지위 요건 적용 결과

통계청 마이크로데이터 통합서비스(MDIS) 공공용 온라인 분석 시스템에서 산출한 '2019년 전국사업체 조사' 결과[14]에 4장에서 제안한 정보보호 최고책임자의 지위 요건을 적용하여 표 5와 같이 업종별·지위별 정보보호 최고책임자 지정 의무 사업체수를 도출하였다. 정보보호 최고책임자의 지위를 이사로 지정해야 하는 사업체는 843개, 임원급으로 지정해야 하는 사업체는 9,684개, 부서장으로 지정해야 하는 사업체는 15,485개로 나타났다.

이 결과로부터 우선 정보보호 전담 조직 구성이 곤란한 종업원 수 50인 미만 기업의 부담 경감 효과를 볼 수 있다. 그리고 1차 산업, 숙박 및 음식점업 등 정보보호 우선도가 낮은 업종과 전기·가스 공급업, 정보통신업 등 정보보호가 중요한 업종에서의 정보보호 최고책임자의 지위 차이로부터 업종별 특성이 반영되었음을 명확하게 알 수 있다. 한편, 국내 정보보호 인력 123,743명 중 정보보호 최고책임자의 자격을 가진 특급 수준의 인력은 27,805명이므로[8], 이 결과가 인력수급면에서도 현행 의무대상인 3.9만여개[9]보다 실효성이 있고 현실적임을 알 수 있다.

12) 2020 정보화통계집[7]의 분류를 따른 것이며, 이는 UNCTAD(1~9명, 10~49명, 50~249명, 250명 이상), OECD(10~49명, 50~249명, 250명 이상)의 기준에 기반하였다.

13) 시행 2019. 1. 1. 금융위원회고시 제2018-36호, 2018. 12. 21., 일부개정 기준. 제8조제2항제1호 "정보기술부문 인력은 총 임직원수의 100분의 5 이상, 정보보호인력은 정보기술부문 인력의 100분의 5 이상이 되도록 할 것"

14) 정보통신서비스 제공자 관련 통계는 발견하지 못하였으나 인터넷을 이용하는 기업체가 99.7%이므로[7] 모든 사업체를 정보통신서비스 제공자로 가정하였다. 조직형태코드가 개인사업체·회사법인인 자료에서 산업대분류코드·종사자합계를 기준으로 집계표를 산출하였다. 전체 사업체수 3,901,561개, 종업원 수 50인 미만 사업체 3,867,108개, 종업원 수 50인 이상 사업체 34,453개.

<표 5> 업종·지위별 정보보호 최고책임자 지정 의무 사업체

| 표준산업분류 \ 지위 | 이사 | 임원급 | 부서장 | 대표자 |
|---|---|---|---|---|
| 농업, 임업 및 어업 | - | - | 2 | 2,248 |
| 광업 | - | - | 1 | 1,759 |
| 제조업 | 119 | 824 | 9,735 | 425,430 |
| 전기, 가스, 증기 및 공기조절 공급업 | 27 | 100 | - | 2,429 |
| 수도, 하수 및 폐기물 처리, 원료 재생업 | - | - | 224 | 8,042 |
| 건설업 | - | 58 | 420 | 145,455 |
| 도매 및 소매업 | 15 | 208 | 2,950 | 1,014,197 |
| 운수 및 창고업 | 193 | 2,825 | - | 402,384 |
| 숙박 및 음식점업 | - | 4 | 50 | 782,472 |
| 정보통신업 | 229 | 1,622 | - | 40,023 |
| 금융 및 보험업 | 176 | 1,537 | - | 29,119 |
| 부동산업 | 3 | 40 | 368 | 142,450 |
| 전문, 과학 및 기술 서비스업 | - | 44 | 271 | 106,062 |
| 사업시설 관리, 사업지원 및 임대 서비스업 | - | 99 | 710 | 69,051 |
| 교육 서비스업 | - | 21 | 358 | 165,490 |
| 보건업 및 사회복지 서비스업 | 75 | 2,278 | - | 107,553 |
| 예술, 스포츠 및 여가관련 서비스업 | 6 | 23 | 387 | 114,886 |
| 협회 및 단체, 수리 및 기타 개인 서비스업 | - | 1 | 9 | 316,499 |
| 합계 | 843 | 9,684 | 15,485 | 3,875,549 |

## 6. 결론

본 논문은 정보보호 거버넌스를 기반으로 정보보호 최고책임자의 법적 지위를 제안하고, 업종별 영향도와 종업원 수에 따라 정보보호 최고책임자의 법적 지위를 차등화한 후, 국가통계를 바탕으로 본 연구의 실효성을 보였다. 본 연구는 정보보호 거버넌스에 따라 정보보호 최고책임자의 법적 지위 요건을 제시하고 그 실효성을 설문이 아닌 국가통계에서의 적용 결과를 바탕으로 보였다는 의의를 가진다.

## 참고문헌

[1] 과학기술정보통신부·한국인터넷진흥원, "정보보호 최고책임자(CISO) 지정·신고 제도 안내서", 2019

[2] 한국사회학회, "정보보호최고책임자(CISO)제도 도입 연구", 한국인터넷진흥원, 2009

[3] International Organisation for Standardization, "ISO/IEC 27014:2020 Information security, cybersecurity and privacy protection − Governance of information security", 2020

[4] 강은성, 홍성권, 백제현, "CISO 길라잡이 기본편", 과학기술정보통신부·한국인터넷진흥원, 2020

[5] 박종섭, 박나룡, 서진원, 강은성, "CISO 길라잡이 중급편", 과학기술정보통신부·한국인터넷진흥원, 2021

[6] 강은성, "CxO가 알아야 할 정보보안", 한빛미디어, 2015

[7] 과학기술정보통신부·한국지능정보사회진흥원, "2020 정보화통계집(국가통계 승인번호 제120008호)", 2020

[8] 과학기술정보통신부·한국인터넷진흥원, "2016년 정보보호 인력수급 실태조사", 2017

[9] 과학기술정보통신부, "정보보호 최고책임자(CISO) 제도개선 6월 13일 시행", 2019