http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.23, No.4, November 2018, pp.87-107
https://doi.org/10.7838/jsebs.2018.23.4.087

국내 금융 사이버보안 규제의 국제경쟁력 제고를 위한 연구: 美 뉴욕 주 금융 사이버보안 규정 (23 NYCRR 500)을 중심으로

A Study on Cybersecurity Regulation for Financial Sector: Policy Suggestion based on New York's Cybersecurity Regulation (23 NYCRR 500)

김도철(Docheol KIM)*, 김인석(Inseok Kim)**

초 록

세계 금융 및 사이버보안 중심지인 미국에서 최초로 제정된 금융부문 사이버보안 규제인 '뉴욕 주 금융 사이버보안 규정(23 NYCRR 500)'이 2017년 3월 뉴욕에서 시행되었다. 기존의 금융 정보보안 법률과 달리 23 NYCRR 500은 위험평가 기반 정책수립, 비공개 데이터의 보안 강화, 정보보안 최고 책임자(CISO) 지명, 내부위험요소 제거, 연간보고 의무 등을 규정함으로써 뉴욕 내 영업활동을 하는 은행, 보험회사 등 모든 금융기관들은 내·외부 위협으로 부터의 안정성을 입증해야 할 책임이 강화되었다. 본 논문은 뉴욕의 새로운 금융 사이버보안 규정과 기존 미국 금융 법률체제를 분석하고 국내 금융부문 사이버보안 규제(전자금융거래법 및 전자금융감독규정)와의 비교분석을 통해 국내 금융서비스 산업의 국제경쟁력 강화를 위한 금융부문 사이버보안 규제 개선 방안을 제시한다.

ABSTRACT

In March 2017, the State of New York became the first state to implement regulation specific to cybersecurity for financial institutions. Unlike previous regulations regarding information security, it has set a minimum requirements to establish cybersecurity program based on risk assessment results, protect Nonpublic Information, designate of CISO, and report to regulatory entity. This paper presents a need for a new cybersecurity policy in Korea by examining newly adopted cybersecurity regulation in the United States. Finally, the paper identify policy suggestions based on the United States's approach as they have successfully implemented the program.

키워드 : 금융보안 국제경쟁력, 뉴욕 사이버보안 규정, 뉴욕 사이버보안 요구사항, 금융 사이버보안, 전자금융감독규정
Cybersecurity Regulation, Information Security, Financial Sector, Regulation on Supervision of Electronic Financial Activities, 23 NYCRR 500, GLBA, FFIEC

* First Author, Graduate School of Information Security, Korea University(kimdo72@korea.ac.kr)
** Corresponding Author, Graduate School of Information Security, Korea University(iskim11@korea.ac.kr)
Received: 2018-09-13, Review completed: 2018-11-20, Accepted: 2018-11-24

1. 서 론

서울과 부산의 글로벌 금융중심지로의 도약은 정부의 오랜 숙원 사업이자 우리나라 금융서비스 산업이 나아가야할 궁극적 목표이다. 정부는 목표 달성을 위하여 2003년 동북아 금융허브 로드맵을 수립하고 2007년 금융중심지의 조성과 발전에 관한 법률을 제정하였다. 그리고 2008년부터 10년 동안 3차에 걸쳐 중장기 금융중심지 기본계획을 수립하고 금융서비스 산업 경쟁력 강화와 금융시장 선진화를 위한 제도 개선 및 인프라 구축을 지속적으로 추진해 왔다[10].

하지만 영국계 컨설팅 기관인 Z/Yen에서 발표한 국제금융센터지수(Global Financial Center Index, GFCI)에 따르면 2018년 서울의 금융서비스 경쟁력 측정지수는 27위로 2016년 대비 15단계나 하락하였고, 외국계 금융회사들은 국내 영업축소 움직임이 확대되면서 2017년에는 7년만에 처음으로 외국 금융회사 진입추이가 감소하였다.

이러한 위기를 타계하기 위해 금융위원회는 2017년 9월 '제4차 금융중심지의 조성과 발전에 관한 기본계획(2017~2019)'을 세우고 2019년까지 금융시장 국제경쟁력 강화를 목표로 ① 자본시장 국제화, ② 금융서비스 산업의 국제경쟁력 제고, ③ 금융시스템의 국제정합성 제고, ④ 금융중심지 내실화 등 4대 과제를 추진하기로 확정하였다. 특히 '금융시스템의 국제정합성 제고' 과제에서는 금융규제의 국제기준 마련을 위해 국제 논의에 적극 참여하여 금융규제의 국제정합성을 제고하고, 원칙 중심(Principle-based)의 금융규제 개편을 추진하기 위한 방안을 제시하였다.

세계적으로 각 국의 전자금융시스템이 고도화되고 상호연관성(inter-connectedness)이 높아짐에 따라 이를 보호하고 안정성을 보증할 수 있도록 금융보안 규제가 재정비되고 있다. 이러한 국제적 흐름에 뒤처지지 않도록 우리나라 또한 금융보안 법률의 발전 및 국제상호운용성을 강화할 수 있는 방안 마련이 시급한 상황이다. 하지만 금융시스템의 국제정합성 제고를 위한 과제에 있어 현재 국내 금융보안 규제에 대한 논의는 제외된 상태이다. 우리나라의 금융보안 규제가 국제적 수준에 부합할 수 있도록 보완・개선할 수 있는 정책이나 제도 마련은 아직도 미비한 편이며 사이버보안의 특성과 목표를 반영한 금융보안 모델 연구 역시 부족한 실정이다.

금융 및 사이버보안 선진국인 미국은 2017년 2월 금융기관을 대상으로 사이버 공격을 예방할 방지책의 일환으로 사이버보안 역사상 가장 엄격하다는 평가를 받고 있는 뉴욕 주 행정규정인 금융 사이버보안 규정(Cybersecurity Requirements for Financial Services Companies)인 23 NYCRR 500을 공포하고 그해 3월 1일에 시행하였다[4]. 세계 금융 네트워크의 상관성이 갈수록 높아지는 현시점에 23 NYCRR 500의 등장은 향후 미국을 포함한 전 세계 금융 사이버보안 체계에 시사하는 바가 크다.

본 논문은 23 NYCRR 500 체계 및 항목별 분석, 기존 미국 금융 정보보안법과 비교, 국내 법규와의 비교분석을 통해 23 NYCRR 500의 사이버보안 목표와 방법론을 분석하고 향후 국내 금융 사이버보안 규제가 국제적 수준의 경쟁력을 갖추기 위한 정책적 대안을 제시하고자 한다.

2. 23 NYCRR 500 규정에 대한 이해

2.1 뉴욕 금융규제의 파급력

뉴욕 금융시장은 이미 미국 내 경제를 좌우할 뿐만 아니라 국제적 단기자금 운용의 시장으로써 세계 금융 자본의 중심적인 역할을 수행하고 있다. 국제금융센터지수에 따르면 뉴욕은 런던과 함께 세계 최고 수준의 금융센터를 보유하고 있으며, 월스트리트의 뉴욕증권거래소(NYSE)와 나스닥(NASDAQ)은 일일 거래량과 시장자본 규모에서 세계 1, 2위로 자리 잡았다[26]. 이에 세계적 금융기관들이 뉴욕 주에 본점, 지점, 현지법인의 형태로 영업망을 집중시키고 있으며 2018년 6월 현재 <Table 1>과 같이 국내 제1금융기관 7개를 포함하여 약 4,400여 개의 금융기관이 영업활동을 위해 '뉴욕 주 금융서비스부(New York State Department of Financial Services, 이하 "NYDFS")'에 등록되어 있다[21].

뉴욕의 금융서비스 산업 규제 품질(Regulatory Quality)은 도쿄와 함께 세계 최고 수준으로 평가받고 있다[26]. 그 결과 뉴욕 금융서비스 산업의 안정성과 건전성을 보장하기 위하여 금융관련 규제체계 마련에 선봉적인 역할을 담당하고 있는 NYDFS의 노력의 성과이기도 하다. 뉴욕 주 정부는 은행, 보험회사 등 금융기관들을 관리·감독할 수 있는 금융규제당국인 NYDFS를 2011년 창립하였으며, NYDFS는 금융서비스법(Financial Law)의 102, 102, 201, 202, 301, 302, 408 섹션에서 부여받은 권한에 따라 뉴욕의 금융기관들을 관리 감독하며 새 규정을 공포할 수 있다[20].

〈Table 1〉 List of Korean Banks Registered to NYDFS

Name of Korean Banks listed in NYDFS	Type of Institution
NongHyup Bank	Foreign Branch
Shinhan Bank America	Bank, Foreign Branch
Woori America Bank	Bank, Foreign Agency
KEB Hana Bank	Foreign Agency
Kookmin Bank	Foreign Branch
Korea Development Bank	Foreign Branch
Industrial Bank of Korea	Foreign Branch

뉴욕 주의 특성상 새로운 금융 사이버보안 규제의 발표는 미국 사이버보안 법률뿐만 아니라 전 세계 주요 금융기관의 사이버보안 정책에 전반적인 영향력을 발휘한다. 첫째, 뉴욕 주에 본점, 지점 및 현지법인을 두고 있는 4,000여 개 이상의 전 세계 금융기관 및 이들과 관련된 제3자 서비스 제공자가 적용 받게 되며 이들 금융기관들은 23 NYCRR 500을 준수하기 위하여 부단히 노력하고 있다. 둘째, 뉴욕 주의 금융관련 법률 및 규정은 미국 전역에 그 파급효과가 크다. 뉴욕주는 자금세탁방지(AML)법, 가상화폐(23 NYCRR 200, Virtual Currencies) 관련 규제 등 지금까지 미국의 금융관련 법률 발전에 선구적인 역할을 해왔으며 이는 다른 주에서 모범사례로 채택되었다[1]. 미국 내 최초로 사이버 공격으로부터 소비자와 금융기관을 보호하기 위한 사이버보안 규정인 23 NYCRR 500에 대한 안전성과 효과가 드러나게 되면 더 많은 기관들과 주정부, 연방정부에서 비슷한 규제를 도입할 것으로 보인다. 미국 보험감독관협의회(National Association of Insurance Commissioners, NAIC)에서는 이미 23 NYCRR 500을 모델로 '보험산업 보안표준(Insurance Data Security Model Law)'을 도입하였으며, 뉴

욕 주 이외 다른 주에서도 23 NYCRR 500을 모델로 한 사이버규정을 도입 중이다[14, 17]. 셋째, 세계적으로 각 산업분야의 정보보호 표준 마련이 대두되면서 유럽연합(EU)의 개인정보 보호 규정(General Data Protection Regulation, GDPR)과 같은 사이버보안 선진국들의 규정이 주목을 받고 있는 가운데, 23 NYCRR 500 또한 금융 사이버보안 분야에 새로운 기준으로 채택될 가능성이 높다.

2.2 NYCRR의 체계

NYCRR은 New York Codes, Rules and Regulations의 약자로 뉴욕 주 정부 기관들의 규정들을 모은 편찬이다[3]. 1945년 처음 발간되었으며 뉴욕 주 정부 기관들은 법에서 부여받은 권한에 한해 규칙과 규정들을 공포하고 NYCRR에 포함시킨다. NYCRR은 실질적으로 입법절차를 밟지 않은 규제이지만 법과 동일한 효력을 발휘한다. NYCRR은 총 23개의 표제(Title)로 구성되어있으며 각 표제를 담당하는 기관과 주제를 <Table 2>에 정리하였다[24]. 이중 표제 23은 금융서비스(Financial Services)로 2011년 이후 뉴욕 주 금융서비스부(NYDFS)가 담당하고 있으며 6개의 Part로 구성되어 있다. 23 NYCRR의 각 Part별 세부 규제는 <Table 3>에서 확인할 수 있다.

따라서 23 NYCRR 500은 뉴욕 주의 금융감독기관인 NYDFS가 공포한 사이버보안 규정으로 모든 금융기관들이 적용대상이 된다. 또한 법과 동일한 효력을 발휘함으로 뉴욕 은행법(Banking Law), 보험법(Insurance Law) 및 금융서비스법(Financial Services Law)에 따라 규정 미이행 시 처벌 대상이 된다.

〈Table 2〉 Title of the NYCRR and its Corresponding Departments

Title	State department
1	Agriculture and Markets
2	Audit and Control (Office of the State Comptroller)
3	Banking
4	Civil Service
5	Economic Development (Empire State Development)
6	Environmental Conservation
7	Correctional Services
8	Education
9	Executive
10	Health
11	Insurance
12	Labor
13	Law(Attorney General's Office)
14	Mental Hygiene
15	Motor Vehicles
16	Public Service
17	Transportation
18	Social Services
19	State(Secretary of State's Office)
20	Taxation and Finance
21	Miscellaneous
22	Judiciary
23	Financial Services

〈Table 3〉 Regulations within Title 23 of NYCRR

Part	Name of Regulation
1	Debt Collection By Third-Party Debt Collectors and Debt Buyers
100	State Charter Advisory Board: Selection Of Candidates Representing Banking Institutions
200	Virtual Currencies
201	Registration Requirements and Prohibited Practices for Credit Reporting Agencies
400	Independent Dispute Resolution for Emergency Services and Surprise Bills
500	Cybersecurity Requirements for Financial Services Companies
501	Nationwide Multistate Licensing System and Registry

2.3 23 NYCRR 500 도입 배경

23 NYCRR 500의 Section 500.00 전문에서 규정의 목적과 도입 배경을 찾을 수 있다. 먼저 NYDFS는 금융기관을 표적으로 한 사이버공격을 면밀히 모니터링 해왔으며 최근에는 취약점을 악용하여 중요한 정보를 탈취하려는 시도를 포착하였다[18]. 2016년 미국 법무부는 2011년부터 2013년 미국 46개 금융기관을 목표(Target)로 한 디도스 공격의 배후로 이란 출신의 해커들을 대거 기소하였으며 이 공격으로 인해 뱅크오브아메리카, JP모건, 뉴욕증권거래소 등이 서비스 장애를 겪었었다[15]. 이후에도 뉴욕 주의 주요 금융기관들이 지속적인 공격에 노출됨에 따라 이들 금융기관들의 보안 수준 제고를 요구하는 목소리가 높아졌다. 일련의 사건들을 통해 NYDFS는 고객정보를 보호하고 금융기관의 정보시스템 보안 수준을 강화하기 위한 작업을 추진하게 된다.

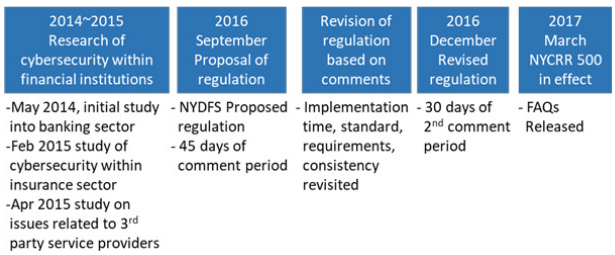
2014년 NYDFS는 뉴욕 주에서 영업활동을 하고 있는 150개 은행을 대상으로 사이버 보안에 관련한 설문을 실시했는데 해당 설문에서 은행들의 제3자 정보제공으로 인한 위험도가 매우 높게 측정되었다[23]. 이후 2차 조사에서는 40개의 은행을 대상으로 제3자 정보제공에 대한 보호대책에 집중하였는데, 이중 오직 35%만이 주기적으로 제3자 제공자에 대한 보안수준 점검을 이행하는 것으로 나타났다. 그 다음해인 2015년 2월에 발표된 “Report on Cyber Security in the Insurance Sector”에 따르면 43개 보험회사의 사이버보안 조사를 실시한 결과 오직 한곳을 제외하고 모든 보험회사들이 위험평가 결과 및 위험을 최소화 할 수 있는 대응책을 제출하지 못했다. 2014년부터 2년에 걸쳐 실시한 조사결과를 토대로 NYDFS는 뉴욕 주 내 금융기관들의 내부통제가 미흡하다는 결론을 내림으로써 2016년 본격적으로 새로운 규정 마련에 착수하게 된다[19].

NYDFS는 2016년 12월 새로운 사이버보안 규정에 대한 제안을 발표하였으며 업계의 150개 이상의 의견서들을 반영해 기준들을 수정하였다. 이에 따른 최종본인 23 NYCRR 500은 16항목의 사이버보안 최소 기준(Minimum Standard) 요구사항으로 구성되게 되었다.

2014년부터의 23 NYCRR 500의 도입 과정을 정리하면 <Figure 1>과 같다.

2.4 23 NYCRR 500 적용대상

뉴욕 주 은행법과 보험법 또는 금융서비스법에 의거해 면허, 등록, 인가, 증명, 허가, 승인, 기타 유사한 허가를 받아 사업을 운영하는 금



〈Figure 1〉 Process of 23 NYCRR 500 Finalizations

융기관들은 23 NYCRR 500의 적용 대상이 된다[18]. 은행, 보험, 외국 법인, 모기지 브로커 등 금융서비스업에 속한 금융기관들이 모두 포함되기 때문에 적용범위가 매우 폭넓다.

단, 다음 중 1개의 조건에라도 해당된다면 16개의 준수사항 중 9개에 대해서 그 의무가 면제된다.

- 종업원 10인 미만
- 3년 회계연도 동안 매출 연간 500만 달러 미만
- 연말 기준자산 1,000만 달러 미만

규제 대상인 금융기관의 주요 정보를 처리, 저장, 전송하는 제3자 서비스 제공자 또한 23 NYCRR 500의 요구사항을 일부 적용 받는다.

2.5 23 NYCRR 500 항목별 분석

23 NYCRR 500은 500.00~500.23까지 24개의 항목으로 구성되어있다. 500.00과 500.01은 서론과 용어의 정의이며 500.02~500.17까지는 규제대상 금융기관들이 준수해야 할 16개의 사이버보안 요구사항을 나열하였다. 500.18~500.23은 기밀보장, 적용면제, 시행일자, 유예기간 등을 다룬다. 각 항목별에 대한 주요 요구사항 정리 및 분석은 다음과 같다[18, 19].

- 500.01(정의) 23 NYCRR 500의 핵심은 프라이버시법(Privacy laws), 미국 의료정보보호법(Health Insurance Portability and Accountability Act, 이하 “HIPAA”) 등 다른 관련법과의 일관성 있는 비공개 정보(Nonpublic Information, NPI)의 정의이다. 비공개 정보는 금융기관이 보유하고 있는 비공개 전자정보이며 23 NYCRR 500에서 보호하고자 하는 정보이다. NPI는 다음을 포함한다.
  ① 사업관련 정보(유출 시 사업, 운영, 보안 등에 중대한 영향을 초래하는 정보)
  ② 개인정보, 사회보장정보, 금융정보(카드번호 등), 계좌 비밀번호, 생체인증정보 등
  ③ 건강 관련 정보(Healthcare Information).
  개인정보, 민감정보 뿐만이 아닌 공개 시 문제를 야기할 수 있는 사내 주요 정보는 모두 NPI로 분류할 수 있다.
- 500.02(사이버보안 프로그램) 위험평가(Risk Assessment)를 통해 해당 금융기관 정보시스템(Information System)의 기밀성, 무결성, 가용성을 보장하는 보안 프로그램을 확립한다.
- 500.03(사이버보안 정책) 정보시스템과 비공개 정보 보호를 위해 사이버보안 정책이 수립되어하며 다음과 같은 내용들이 정의 되어야 한다: (a) 정보 보안 (b) 데이터 관리 및 분류 (c) 보유 자산 및 장비 관리 (d) 접근 통제 및 신원 관리 (e) 사업 연속성 및 재난 복구 계획 및 자원 (f)시스템 운영 및 가용성 문제 (g) 시스템 및 네트워크 보안 (h) 시스템 및 네트워크 모니터링 (i) 시스템 및 애플리케이션 개발과 품질 보증 (j) 물리적 보안 및 환경 통제 (k) 고객 정보 보호 (l) 공급업체 및 제3자 서비스 제공자 관리 (m) 위험평가 (n) 사고 대응
- 500.04(정보보안 최고 책임자) 사이버보안 프로그램의 감독 및 시행을 책임질 수 있는 자격을 갖춘 개인(이하 “정보보안 최고 책임자” 또는 “CISO”)를 지정한다. CISO는 대상 금융기관 소속이거나 금융

기관 소속이 아닌 제3자 업체로부터 고용 가능하다. 임명된 CISO는 경영진에 연 1회 이상 사이버보안 프로그램 및 보안 위험에 대해 서면으로 보고를 할 의무를 지닌다.

- 500.05(모의침투 테스트 및 취약성 평가) 각 금융기관은 지속적인 모니터링을 실시한다. 지속적인 모니터링이 불가능하다면(위험평가에 따라 식별된 위험에 기초하여) 매년 금융기관의 정보시스템에 대한 침투 테스트를 진행하고 2년마다 취약성 평가를 실시한다.
- 500.06(감사 추적) 금융거래내역은 최소 5년간 보유해야 하며, 사이버보안 사건(Event)은 최소 3년간 보관해야 한다.
- 500.07(접근 권한) 비공개 정보에 대한 접근을 제공하는 정보시스템에 대한 사용자 접근권한을 제한하고, 접근권한을 주기적으로 검토해야한다.
- 500.08(응용프로그램 보안) 안전한 응용프로그램 개발을 보장하기 위한 절차, 가이드라인, 표준이 마련되어야 하며 이를 평가하고 테스트할 수 있어야 한다. 이 조항은 제3자가 개발한 프로그램에도 적용된다.
- 500.09(위험평가) 정보시스템에 대해 주기적으로 위험평가를 수행해야 한다. 이는 문서화된 정책과 절차에 따라 수행된다. 위험평가는 금융기관의 기술적 운영방안과 사이버 정책 수립에 있어 핵심적인 역할을 한다. 식별된 위험에 대해서 각 금융기관은 이를 어떻게 완화하고 해결할 것인지 구체적으로 기술하여야 한다.
- 500.10(사이버보안 및 정보보호 인력) 자격을 갖춘 CISO 지정 외에도 사이버보안 위험을 관리하고 수행할 보안전문인력을 확보하여야 한다. 또한 사이버보안 인력이 새로운 보안위협에 대응하고 최신 기술을 습득할 수 있도록 교육 기회를 제공해야 한다.
- 500.11(제3자 서비스 제공자 보안정책) 각 금융기관은 제3자 서비스 제공자를 식별하고 위험평가를 실시해야 한다. 또한 제3자 제공자의 정보시스템, 비공개 정보 접근에 대한 정책 및 절차를 수립하여야 한다. 그러한 정책은 각 금융기관의 위험평가에 기반을 두고 있어야 한다.
- 500.12(다중 인증) 정보시스템 및 비공개 정보에 대한 비인가 접속을 방지하기 위해 다중-요소 인증(Multi-Factor Authentication) 또는 위험-기반 인증(Risk-Based Authentication)을 적용해야 한다. 특히 외부 네트워크에서 내부 네트워크로 접속하는 모든 사용자는 다중 요소 인증이 무조건 적용된다. 위험기반 인증은 위험지수를 기반으로 인증 요건이 강화되는 기술이다. 예로, 비정상적으로 의심되는 접근에 대해서는 추가 인증을 요구하게 된다.
- 500.13(데이터 보유제한) 법률에서 요구하는 정보를 제외하고는 사업 목적을 달성하거나 불필요해진 비공개 정보는 안전하게 파기하여야 한다.
- 500.14(훈련 및 모니터링) 인가된 사용자에 대한 활동 감시 및 비인가자의 무단 접근을 탐지하기 위한 정책, 절차, 통제를 구축해야 한다. 위험평가에서 식별된 위험을 반영한 사이버보안 훈련을 모든 인력을 대상으로 실시한다.

- 500.15(비공개 정보 암호화) 네트워크를 통해 전송되거나 사내에 보유하고 있는 비공개 정보는 모두 암호화해야 한다. 비공개 정보의 암호화가 불가능한 경우 CISO의 승인 하에 비공개 정보를 보호할 대체방안을 마련할 수 있다.
- 500.16(침해사고 대응계획) 각 금융기관은 사이버보안 사고 대응 및 신속한 복구를 위한 계획을 서면으로 작성해야 한다. 특히 신속한 복구를 위한 구성원의 역할과 책임(Role and Responsibilities)을 명확히 정의한다.
- 500.17(감독기관 보고) 각 금융기관은 다음과 같은 사항을 감독기관에 보고할 의무를 가진다.
  ① 연간 규정 준수 확인서(annual certification of compliance)를 매년 2월 15일까지 NYDFS 포털을 통해 제출해야 한다. 확인서에는 금융기관 이사장의 서명이 포함되어야 하며 확인서와 관련된 모든 기록, 일정, 증적자료는 최소 5년간 보관해야 한다.
  ② 각 금융기관은 사이버보안 사고가 발생한 것으로 판단되는 경우 72시간 내 감독기관을 포함한 관련 정부기관들에 보고해야 한다.

23 NYCRR 500의 모든 항목은 위험평가에 기반하여 수립・적용된다. 따라서 각 금융기관은 1차적으로 비공개 정보 및 정보시스템을 고려한 주기적인 위험평가를 수행하고 이후 도출된 결과를 통해 금융기관이 당면한 보안 위험 최소화를 위한 사이버보안 프로그램을 정의한다. 추가적으로 CISO의 임명, 교육, 침투 테스트 및 취약성 평가, 비공개 정보의 암호화, 감사 로그 보관 같은 최소한의 관리적 및 기술적 보호조치를 요구하고 있다.

2.6 처벌기준

뉴욕 주 금융 사이버보안 규정인 23 NYCRR 500 원문에는 처벌에 관련한 조항이 없다. 다만, 해당 규정의 Section 500.20에 따르면 “감독원장이 권한으로 관련법령에 의거하여 집행할 수 있다”라고 쓰여 있다[18].

이에 관한 제재 법령 근거는 뉴욕은행법(New York Banking Law), 뉴욕보험법(New York Insurance Law) 및 뉴욕금융서비스법(New York Financial Services Law)에서 찾을 수 있다.

뉴욕은행법 § 44에 따르면 컴플라이언스 위반 시 NYDFS가 가할 수 있는 벌금형은 다음과 같다.

1) 위반사항이 발견된 후 시정하지 않을 경우 최대 일일 $2,500 벌금
2) 본점(지점이 아님) 자산규모의 최대 1%
3) 은행 자회사들 자산규모의 최대 1%

이외에도 행정제재(Consent Order)를 가할 수 있으며, 사안이 심각할 경우 뉴욕 주의 은행 라이선스를 취소(License Revocation)할 수 있다.

NYDFS는 자금세탁방지 컴플라이언스 위반 사항에 대해서 천문학적인 벌금을 부과한 적이 있으며 최근 BNP 파리바, 도이치뱅크, 크레디트스위스 등 외국계 은행뿐만 아니라 한국계 은행에 대해서도 순차적으로 징계하였다[2]. 23 NYCRR 500 또한 NYDFS가 담당하고 있으므로 해당 규정 위반으로 인한 처벌기준은 자금세탁방지와 동일하게 적용될 가능성이 높다.

3. 기존 미국 금융보안 법률과의 비교

23 NYCRR 500을 적용받는 뉴욕의 금융기관들은 이전부터 금융서비스 현대화법(Gramm-Leach-Bliley Act, 이하 “GLBA”)와 연방금융기관검사위원회(Federal Financial Institutions Examination Council, 이하 “FFIEC”)에서 작성한 IT 감사 매뉴얼(IT Examination Handbook)을 준수해왔다. 금융서비스 산업 사이버보안의 표준이 되어온 기존 규제들의 이해를 통해 23 NYCRR 500의 중복 규정 여부와 차이점을 비교분석하여 갭을 도출해 보고자 한다.

3.1 금융서비스 현대화법(GLBA)과의 비교

금융서비스현대화법(GLBA)는 금융기관이 보유하고 있는 개인신용정보보호에 관한 연방법으로 1999년 제정되었다[22]. 이 법은 은행의 증권업무 취급 제한을 폐지하고 은행과 증권사의 합병을 허용한 법으로 알려져 있다. 또한 잇달아 발생한 금융기관들의 무분별한 고객정보 오남용 및 유출 사고들을 억제하기 위한 방안으로 개인신용정보의 보호조치를 의무화한 것으로 유명하다.

GLBA에서 핵심이 되는 개념은 비공개 개인정보(Nonpublic Personal Information)이다. 여기서 비공개 개인정보란 <Table 4>에 정의된 바와 같이 금융고객의 개인식별정보, 거래정보 등으로 공개적으로 입수되지 않은 개인정보를 말한다. 금융기관은 비공개 개인정보 보호와 제3자와의 공유 제한을 위해 모든 주의를 기울여야 한다.

〈Table 4〉 GLBA Nonpublic Personal Information Definition

GLBA Nonpublic Personal Information
1. (Personal Identifiable Information) Names, addresses, phone numbers, social security numbers
2. (Personal Financial Information) Bank account numbers, credit card numbers

GLBA가 금융 정보보안의 표준으로 거듭나게 된 이유는 미국 연방거래위원회(United States Federal Trade Commission, 이하 “FTC”)가 GLBA 준수를 위한 보호조치 기준(Safeguard Rule)에 비공개 개인정보의 보호를 위한 보안사항 준수 의무를 처음으로 명시하였기 때문이다[15, 22]. 해당 규정에서 금융기관은 서면으로 작성된 보안계획(Written Information Security Plan) 수립, 책임자 임명, 고객정보 대한 위험평가 수행, 접근통제 등을 통해 개인신용정보의 유출 및 도용을 방지하기 위한 금융기관의 보호의무를 강화하였다[8]. 기존 GLBA를 준수하는 금융기관은 23 NYCRR 500과 GLBA의 보안프로그램 확립, 위험평가 수행, 고객정보 접근통제, 보안 담당자 임명 부분에서 중복 적용을 받는다[25].

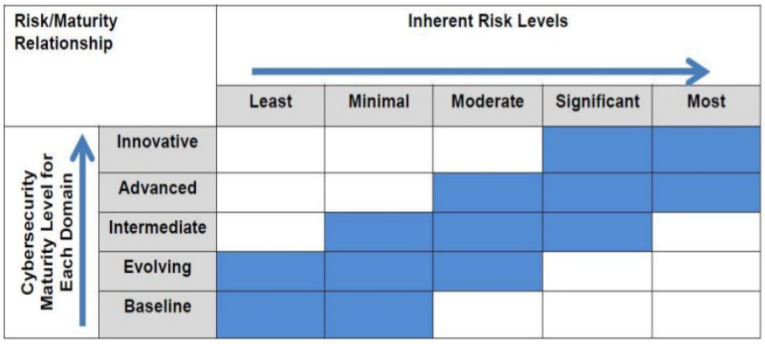
표면적으로 보았을 때 GLBA와 23 NYCRR 500은 유사점이 많으나 서로 다른 목표와 특징을 가지고 있다. 첫째로, GLBA는 정보 중심의 보안인 반면 23 NYCRR 500은 사이버보안 전반을 아우른다. FFIEC는 정보보안(Information Security)과 사이버보안(Cyber Security)을 다르게 정의하고 있는데, 정보보안이란 “정보의 생성, 수집, 보유, 전송, 파기까지의 전 과정 및 정보를 보유 및 전송하는 하드웨어와 인프라 보호”를 뜻하는 반면에 사이버보안이란 “사이버

공격의 방어(Prevent), 탐지(Detect), 대응(Response)을 통해 고객과 기관의 정보를 보호하는 것을 목표로 한다[7]. GLBA는 1999년 금융기관의 고객정보 오남용을 억제하고 이를 보호할 의도로 제정된 법으로 사이버보안을 목표로 하고 있지는 않다. FTC의 GLBA 준수를 위한 보호조치기준 원문에는 “고객정보의 기밀성과 무결성 보장을 위한 관리적, 기술적, 물리적 조치”를 언급하고 있으며 네트워크를 포함한 정보시스템의 외부공격 대응에 대한 언급은 없다[25]. 반면, 23 NYCRR 500은 정보뿐만이 아닌 정보시스템 전반에 대한 보호조치를 의무화함으로써 금융기관의 사이버보안 강화를 최종 목표로 삼았다. 둘째로, 23 NYCRR 500은 보호가 필요한 정보 범위를 넓힘으로써 금융기관이 관리해야 할 보안 영역을 확대하였다. GLBA는 개인식별 정보(Personally Identifiable Information)과 신용정보의 보호에만 적용되었고 이외 건강정보 등은 관리감독 대상에서 배제되었다. 2017년 이전으로 건강정보를 보관하고 있는 금융기관들은 보건부(Health and Human Services) 관리대상으로 미국 의료정보호법(HIPAA)의 보안 기준을 적용 받았다. 23 NYCRR 500은 기존 GLBA의 비공개 개인정보(Nonpublic Personal Information)에 사업관련 정보와 건강정보를 포함하여 보호대상이 되는 정보 및 정보시스템을 확대함으로써 금융기관 내 일관된 보안정책 적용을 도모하였다.

3.2 연방금융기관검사위원회(FFIEC) IT 감사 매뉴얼과 사이버보안 평가 도구

미국은 1979년 금융기관 규제 및 금리제한법(Financial Institutions Regulatory and Interest Rate Control Act)에 따라 FFIEC라는 조직을 설립하여 금융기관 전반에 표준화된 기준을 적용하기 시작했다[5]. FFIEC는 5대 금융감독기관인 연방준비이사회(Federal Reserve Board), 연방예금보험공사(Federal Deposit Insurance Corporation), 통화감독청(Office of the Comptroller of the Currency), 소비자 금융 보호국(Consumer Financial Protection Bureau)으로 구성되어 있다. FFIEC는 금융기관의 법률 준수를 돕기 위해 11개의 소책자로 구성된 IT 감사 매뉴얼(Information Technology Examination Handbook)을 발간하였는데 이 책자는 IT 관리, 운영, 결제 시스템, 감사 등의 내용을 포함하고 있다. IT 감사 매뉴얼은 GLBA 준수 여부를 판단하기 위한 기준으로써 기관의 감사자들이 우선적으로 참고하는 매뉴얼이다[7, 13]. IT 감사 매뉴얼은 법률 준수를 위한 도구로써 보다 세부적인 조치를 기술하였다. 다만 법률적으로 명시한 요구사항이 아니기 때문에 금융기관들은 어디까지나 IT 감사 매뉴얼을 비법령 규제로 인식해 인용하고 있으며 금융기관별로 서로 다른 형태의 기준이 적용될 수 있다.

23 NYCRR 500은 IT 감사 매뉴얼과 함께 2015년 1월 FFIEC에서 발간한 사이버보안 평가 도구(Cyber Security Assessment Tool)을 적극적으로 활용하도록 권고하고 있다[16]. FFIEC의 사이버보안 평가 도구는 미국 표준기술연구소(National Institute of Standards and Technology, 이하 “NIST”)에서 발간한 Cybersecurity Framework를 토대로 작성되었으며 이 문서는 금융기관의 사이버보안 성숙도(Cybersecurity Maturity)를 객관적으로 평가하고 각 금융기관의 상황에 맞는 정책 수립 및 기술적 보호조치를 적용할 수 있도록 도와준다[6]. 문서에 따르면 사이버 위험



〈Figure 2〉 Cybersecurity Risk/Maturity Relationship in FFIEC Cybersecurity Assessment Tool

도가 높게 측정될수록 금융기관의 사이버보안 수준 또한 높아져야 한다. <Figure 2>는 FFIEC의 사이버 평가 도구 문서에서 발췌한 내용으로 위험도와 금융기관의 사이버보안 성숙도를 매핑한 자료이다. 내재된 위험 수준(Inherent Risk Levels)이 높을수록 금융기관은 보다 높은 사이버보안 성숙도(Cybersecurity Maturity Levels)를 갖춰야 하며, 반대로 위험이 낮을수록 사이버보안 수준도 낮아진다. 이는 각 금융기관의 위험 현황에 맞추어 보안수준을 재정립하고 보안이 취약한 부분에 집중 투자할 수 있도록 가이드한다.

23 NYCRR 500을 적용받는 뉴욕 주의 금융기관들은 사이버보안 평가 도구를 활용하여 위험평가를 실시하고, IT 감사 매뉴얼을 통해 보안 기술을 적용하게 되었다.

3.3 기존 미국 금융보안 법률과의 차이점

23 NYCRR 500은 GLBA와 FFIEC의 IT 감사 매뉴얼과 비교하여 3가지 차이점을 가진다. 첫째, 기존 정보보안에서 사이버보안으로 그 범위가 확장되었다. 기존의 비공개 정보의 기밀성과 무결성 원칙을 유지함과 동시에 사이버 공격의 방어(Prevent), 탐지(Detect), 대응(Response)을 통해 금융기관의 시스템 전반을 보호해야 한다. 둘째, 23 NYCRR 500은 최소 기준(Minimum Standard)의 보안조치 사항을 정의함으로써 보다 규범적이다. 뉴욕 주의 금융기관들은 규정에서 요구하는 바에 따라 특정 기준치(Baseline)에 상응하는 보호조치를 적용해야 한다. 마지막으로, 23 NYCRR 500은 연간 규제기관에 준수여부를 보고하는 체계를 갖춤으로써 감독기관의 규제권한을 강화하였다. 미국은 전통적으로 자율적인 사후적 책임을 원칙으로 금융보안에 대해 네거티브 규제 방식을 적용해왔다. 하지만 23 NYCRR 500은 사이버 침해에 대한 예방차원으로 보고 체계를 도입함으로써 사전적인 규제에 초점을 맞추었다. 따라서 23 NYCRR 500은 기존 금융보안법과 달리 미국 사이버보안 역사상 가장 엄격하고 강력한 규제로 평가되고 있으며, 향후 미국 사이버보안 규제에 새로운 패러다임을 제시할 가능성이 높다.

4. 국내 법규와의 비교

국내 금융기관은 전자금융거래법, 전자금융감독규정, 신용정보의 이용 및 보호에 관한 법률, 개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률을 적용받고 있다. 이중 전자금융거래법 및 전자금융감독규정은 금융기관을 대상으로 한 특별법으로써 23 NYCRR 500의 비교대상으로 선정하기 적합하다.

4.1 전자금융거래법 및 전자금융감독규정과의 비교

우리나라는 각 금융업법에서 요구하는 IT 및 전자금융거래에 대한 관리 감독은 전자금융업무 감독규정 및 시행세칙에 따라 운영되어 왔으나 2007년 1월 전자금융거래법의 제정・시행 및 전자금융감독규정을 통해 일관된 금융기관의 IT 보안 규제체계가 마련되었다[11]. 전자금융감독규정에 따라 우리나라의 금융기관은 일관된 보안정책 및 보호조치를 적용하고 있으며 금융위원회 산하 특수법인인 금융감독원의 관리 감독을 받고 있다. 전자금융감독규정은 23 NYCRR 500 대비 매우 구체적으로 명시되어 있으며 단말기 보호대책, 홈페이지 보안, 망분리, 해킹 방지 대책 등 23 NYCRR 500이 포함하고 있지 않은 보안요구사항들을 전반적으로 다루고 있다. 23 NYCRR 500의 500.02~500.17 조항의 16개의 준수 요구사항과 전자금융거래법 및 전자금융감독규정의 비교를 <Table 5>에 정리하였다.

선언적인 문구로 보았을 때 전자금융거래법 및 전자금융감독규정은 23 NYCRR 500의 보안요구사항을 모두 다루고 있어 보이나 국내법과 23 NYCRR 500은 주요 부분에서 4가지 차이점이 존재한다. 첫째, 23 NYCRR Part 500은 뉴욕 금융서비스 부문이 현재 직면하고 있는 문제를 해결하기 위하여 사이버보안 활동에 대한 최소 규제 기준을 설정한 반면 전자금융거래법 및 전자금융감독규정은 규제 집행의 실효성 확보를 위하여 구체적이고 세세한 내용으로 규제를 명확히 하고 있다. 둘째, 23 NYCRR 500은 위험평가 수행 결과를 토대로 보안 요소를 확립한다. 이는 각 금융기관이 위험요소를 확인하고 대응할 수 있는 전략을 직접 마련할 수 있게 한다. 반면, 전자금융감독규정은 체크리스트 방식으로 금융기관마다 일관된 보안정책과 기술적 보호조치를 적용한다. 셋째, 뉴욕 주의 금융기관들은 23 NYCRR 500 준수를 위해 위험평가를 기반으로 실제 수행한 '사이버보안 활동 보고서'를 감독기관에 보고한다. 반면, 국내 금융기관들은 전자금융거래법 및 전자금융감독규정 준수를 위해 '정보기술부문계획서'와 '전자금융기반시설의 취약점 분석, 평가 결과서'만 감독기관에 제출・보고한다. 특히, 23 NYCRR 500은 비공개정보를 정의하고 그 정의에 따라 보호대상이 되는 정보시스템을 식별하여 취약점 분석 및 평가를 진행하는 방식으로 금융시스템 전반에 대한 취약성 점검을 수행하지만, 국내의 경우 취약점 분석 및 평가를 전자금융기반시설에 한하여 실시하며 그 대상 금융기관 또한 총자산이 2조 원 이상이고 상시 종업원 수가 300명 이상인 금융회사 또는 전자금융업자 등으로 한정하고 있다. 넷째, 모든 뉴욕 주의 금융기관은 제3자 서비스 제공자도 CISO로 임명될 수 있지만 전자금융거래법은 내부(In-house) 임직원만 CISO로 임명될 수 있다.

〈Table 5〉 Comparative Analysis of 23 NYCRR 500 and Information Security Laws for Financial Sector in South Korea

23 NYCRR 500		Electronic Financial Transactions Act[A]/ Regulation on Supervision of Electronic Financial Transactions[R]	
500.02(Cybersecurity Program)	Establish cybersecurity program based on risk assessment results.		N/A
500.03(Cybersecurity Policy)	Establish cybersecurity policies.		N/A
500.04(CISO)	Required to designate CISO. CISO is position, not a title. If appropriately qualified, CISO can be outsourced to a third party.	[A] Article 21-1(Designation of CISO)	CISO designation based on total capital, number of employees, and size. CISO must be C-level employee. Cannot hold other IT positions.
500.05(Penetration Testing & Vulnerability Assessments)	Conduct annual penetration testing. At least bi-annually conduct vulnerability assessment.	[A] Article 21-3(Vulnerability Analysis & Assessment of facility)	Based on total capital, number of employees and size. Annually conduct vulnerability analysis and assessment.
500.06(Audit Trail)	Financial transactions kept for at least 5 years, and cybersecurity events kept for 3 years.	[A] Article 22(Electronic Transaction generate, preserve, retention)	Financial transactions kept for 5 years upon generation. No requirement to preserve cybersecurity events.
500.07(Access Controls)	Adopt effective access controls to protect against unauthorized access to NPI.	[R] Article 14(Information Processing System Protection	Monitoring user access, access logs, activity logs, etc regarding information processing system and its OS.
500.08(Application Security)	Written documentation for secure in-house development practices such as procedures, guidelines, standards.	[R] Article 20(Information processing system deployment), Article 29(Application Control)	To secure the safety and reliability of information processing system, secure practices applied from design to development. Application registration, modification, deletion must proceed according to the procedure. Keep Documentation of maintenance. Application related to electronic transaction must pass the security verification.

〈Table 5〉 Comparative Analysis of 23 NYCRR 500 and Information Security Laws for Financial Sector in South Korea (Continued)

23 NYCRR 500		Electronic Financial Transactions Act[A]/ Regulation on Supervision of Electronic Financial Transactions[R]	
500.09(Risk Assessment)	Conduct periodic risk assessment on information system. This is important for the holistic cybersecurity program.		N/A
500.10(Cybersecurity Personnel and Intelligence)	Utilize qualified cybersecurity personnel and provide them with updates and trainings.	[R] Article 8(Personnel, organization, budget)	[5・5・7 regulation] IT personnel comprised of 5%(or more) of total employees. Information security personnel should be 5%(or more) of IT personnel. Information security budget comprised of 7%(or more) of total IT budget. budget.
500.11(Third Party Service Provider Security Policy)	Identification and risk assessment of 3rd party service providers. Evaluation of cybersecurity practices for 3rd party service providers.	[R] Article 60 (Standards for outsourcing, etc.)	Physical and logical control applied to outsource entity. Use of private lines, and prevention of customer data loss and disruption of information system, etc.
500.12(Multi-Factor Authentication.)	To protect against unauthorized access to NPI or information system, use multi-factor authentication or risk-based authentication.	[R] Article 14(Information Processing System Protection)	Extra authentication procedure required when accessing Operating System of information processing system.
500.13(Limitations on Data Retention)	Secure disposal NPI that is no longer necessary.	[A] Article 22(Electronic Transaction generate, preserve, retention)	Electronic transaction records that are out of date or no longer necessary need to be disposed.(For personal information, it should be disposed accordance to Personal Information Act Article 21)
500.14(Training and Monitoring)	Monitor the activity of Authorized Users and detect unauthorized access. Provide regular cybersecurity awareness training.	[R] Article 13(Electronic Data Protection), Article 19-2(Information Security Education)	For input, output, access of electronic data, user must access according to its use. Information processing system access control. To increase competency of information security, a necessary to set annual education program.(Number of hours may vary for employee status)

〈Table 5〉 Comparative Analysis of 23 NYCRR 500 and Information Security Laws for Financial Sector in South Korea (Continued)

23 NYCRR 500		Electronic Financial Transactions Act[A]/ Regulation on Supervision of Electronic Financial Transactions[R]	
500.15(Encryption of Nonpublic Information)	Encryption of NPI that is held or transmitted.	[R] Article 17(Website, Web Servers, etc Protection, Article 32, 33(Password Management)	Customer information or critical information stored in DMZ must be encrypted. PW of employees or customers stored in information processing system and electronic data must be encrypted.
500.16(Incident Response Plan)	Incident response and recovery plan. Define R&R.	[R] Article 15(Protection from hacking), Article 23(Plan and Operate Incident Response)	Plan incident response and prevention against hacking Planning prevention against Natural disaster, human error, technical disaster, electronic disaster. Plan and operate recovery.
500.17(Notices to Superintendent)	Notice of cybersecurity event to the superintendent no later than 72 hours. Submit annual compliance certification to the superintendent.	[A] Article 21-5(Notice of Incident) [R] Article 37-4(Incident Response Entity and its Role)	Notice to National Financial Committee without delay. Submit Incident response and recovery training plan to head of appropriate organization.

5. 국내 금융 사이버보안 규제의 국제 경쟁력 확보를 위한 대안 및 개선사항

23 NYCRR 500이 금융 사이버보안 규제로써 가지고 있는 특성을 파악하고 국내 금융 사이버보안 규제의 국제경쟁력 확보를 위한 대안을 제시하고자 한다.

5.1 최소 기준의 적용(Minimum Standard)

NYDFS는 23 NYCRR 500의 초안을 작성하기 전 뉴욕 주에서 영업활동을 하고 있는 150개 이상의 금융기관 조사를 통해 보안조치가 필요한 항목들을 정리하였고, 그 결과 사이버 보안 프로그램의 확립, CISO 임명, 모의침투테스트 시행, 비공개 정보 암호화, 다중인증 적용 등의 최소 규제항목들이 도출되었다. NYDFS는 이 항목들을 사이버보안에 있어 없어서는 안 될 핵심원칙으로 지정하는 동시에 “금융서비스 산업의 혁신을 저해하지 않으며, 신기술을 적극적으로 수용할 수 있는 규제의 유연성을 유지”하려 했다[14, 18]. 실제로 23 NYCRR 500은 구체적이고 세부적인 요구사항들은 나열하지 않았으며, 암호화나 다중인증 요소 같은 보호조치는 CISO 승인 하에 동등한 기술조치 시 대체

가 가능하게 하였다. 이는 과학기술 발달에 따르는 금융서비스 산업의 활성화와 기술발전을 저해하지 않는 전통적인 미국의 규제체계를 반영한 것이다.

반면, 국내 현행법은 정보보안에 있어 비교적 강도 높은 수준에서 엄격하고 세부적인 보호조치를 요구함으로써 금융회사들이 신기술 도입을 기피하고 보수적인 자세를 취하도록 하였다. 대표적인 예로 지금까지의 금융권 클라우드 도입은 해킹 등 보안위협을 원천 봉쇄하기 위한 물리적 망분리 규정으로 인해 무산되어 왔었다. 전자금융감독규정 제11조 제11호 및 제12호, 제15조 제1항 제5호는 국내 금융기관 전산실의 국내 설치와 정보처리시스템의 내부망과 외부망의 분리조치를 요구하였으며 이에 따라 금융권의 클라우드 도입은 전자금융감독규정 위반행위로 간주되었다[12]. 2016년 10월 금융위원회는 클라우드 도입과 관련된 조항을 일부 개정하여 비중요정보처리시스템으로 그 범위를 한정하였고, 2018년 7월에서야 개인신용정보를 처리하는 시스템도 클라우드를 도입할 수 있도록 확대하였다[9]. 미국은 이미 2011년부터 금융권에 클라우드를 도입하여 차세대 IT시스템을 구축하였고 이를 기반으로 경쟁력 있는 금융상품들을 출시하였다. 현행 전자금융거래법은 검증된 기술조차 도입을 허가하기 어려울정도로 규제의 기준이 매우 엄격하다. 금융 사이버보안 규제의 최소 기준 적용은 국내 금융서비스 산업의 기술혁신을 불러올 것이며 외국계 금융기관들의 국내시장 진입장벽을 낮춰 동북아 금융중심지로 드높이는데 일조할 것이다.

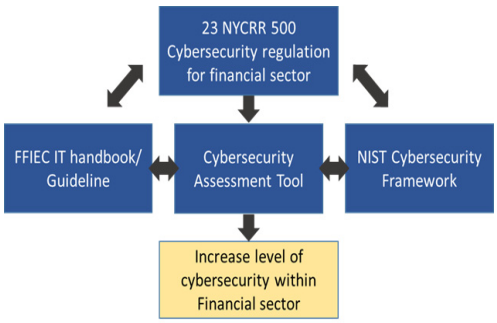
23 NYCRR 500의 최소 기준 적용은 금융 사이버보안 수준의 강화와 금융기술 발전에 장애요소를 제거하는 복합적인 목적을 반영하였다. 우리나라 현행법 또한 최소 기준 적용을 고려하여 금융기관들이 정보통신 기술을 적극적으로 활용하고 동시에 국제경쟁력 강화와 소비자 편익증진을 실현할 수 있도록 입법 방안을 모색하여야 한다.

5.2 위험평가(Risk Assessment) 기반의 접근

전자금융감독규정은 2007년 1월 시행 후 10년간 17번에 걸쳐 개정되어 왔다. 예컨대, 2013년에는 금융 IT 보안을 근본적으로 향상시키기 위한 목적으로 망분리를 의무화하였고, 2015년에 자율보안체제 정착을 지원하고 혁신을 도모하고자 사전 보안성심의 제도와 공인인증서 의무사용 규제를 전면 폐지하였다. 지금까지 전자금융감독규정은 이처럼 일부 조항들의 지속적인 수정을 통해 규제 강화와 완화를 반복하는 사건의존적(Event-based)인 경향을 띄고 있으며, 금융보안법으로써 궁극적으로 갖추어야할 사이버보안의 방향성은 제시하지 못하였다.

23 NYCRR 500은 위험평가를 토대로 금융기관의 사이버보안 수준을 진단하고 각 금융기관에 맞춤화(Tailored)된 사이버보안 프로그램의 확립을 목표로 하고 있다. 또한 주기적인 점검을 통해 금융기관이 진화하는 최신 위협에 대해 유기적으로 대응할 수 있는 체계를 구축하도록 유도한다[16]. 23 NYCRR 500의 모태는 NIST의 Cybersecurity Framework이며 이 프레임워크의 구현은 금융기관이 처한 위기관리 사항, 위협 환경, 법률 및 규제 요건, 사업목적에 따라 사이버보안 위험방식을 적용하도록 단계별로 제시한다.

23 NYCRR 500의 위험평가 방식은 다음과 같은 장점을 가지고 있다. 첫째, 각 금융기관이 자신에게 맞춤화된 사이버보안 정책을 실시함으로써 가장 취약한 부분에 리소스가 집중되도록 한다. 이로써 금융기관들은 평준화된 사이버보안 수준에서 탈피하고 과도한 보안 예산 편성에서 벗어날 수 있다. 둘째, 혁신적인 금융 사이버보안 프로그램 개발을 장려한다. 위험평가 모델에서는 혁신적이고 창의적인 사이버보안 체계 구축을 장려하고 있으며 이는 모범사례의 확산으로 이어질 가능성이 높다. 셋째, 사이버보안 전문기관(미국의 경우 NIST)의 보안 방법론을 기초로 하여 규제의 효과성이 입증되었으며 향후 사이버보안 사건 발생 시에도 전문기관과의 공동대응 차원에서 충격을 완화해 나갈 수 있다. <Figure 3>에 23 NYCRR 500의 모델과 유관 기관들의 관계들을 정리하였다.



〈Figure 3〉 Relationship between Cybersecurity Regulation and its Related Organizations

국내 금융 사이버보안 법률로 대표되는 전자금융감독규정은 독립적인 사이버보안 규제가 아닌 “전자금융”에 대한 규제 체계이며 사이버보안이외에도 약관교부 방법 및 관련 보고, 전자금융업의 허가와 등록 및 업무 등 사이버보안과 관련도가 낮은 항목들도 포함되어있다. 더 나아가 현행법은 검증된 사이버보안 모델을 기초로 하고 있지 않으며 정부의 정책기조에 따라 매번 개정되고 변화되고 있다.

우리나라의 금융 사이버보안 규제가 국제상 호운용성을 확보하기 위해서는 위험평가에 기반한 검증된 사이버보안 프레임워크를 기초로 법이 정립되어야 하며, 국내 사이버보안 전문기관들과 협력하여 새로운 기술, 새로운 위협에서도 규제가 일관성 있게 적용되도록 확고한 로드맵을 제시할 필요가 있다.

5.3 사이버보안의 효과적인 규제 및 감독을 위한 감독기관 보고 대상 및 범위 강화

23 NYCRR 500은 사이버 침해를 방지하고 예방하기 위하여 각 규제대상 금융기관이 CISO를 지정하도록 요구하고 있다. 지정된 CISO는 담당하고 있는 금융기관의 사이버보안 체계 강화를 위하여 수행한 활동 내역이 포함된 연간 규정 준수 확인서(annual certification of compliance)를 감독기관에 보고하도록 되어 있다.

1) 모의침투 테스트
2) 감사 추적
3) 응용프로그램 개발의 보안
4) 주기적인 위험평가
5) 다중인증과 암호화

우리나라의 전자금융거래법 역시 23 NYCRR 500과 마찬가지로 CISO 지정과 감독기관 보고의무를 포함하고 있지만 정보보안 활동과 관련된 보고 의무는 23 NYCRR 500 대비 그 범위가 상대적으로 좁다. 우리나라 금융기관이 감독기관인 금융위원회 또는 금융감독원에 보고해야 하는 내용은 다음과 같다:

1) 정보기술부문 계획서
2) 전자금융기반시설의 취약점 분석, 평가 결과서
3) 정보기술부문 및 전자금융사고 보고

현행법상 국내 금융기관들은 문서화된 계획서만 제출하는 반면에 23 NYCRR 500 규제대상 금융기관들은 사이버 공격으로부터 소비자와 금융기관을 보호하기 위하여 실제 수행한 활동 확인서를 제출함으로써 계획 이행 여부에 대한 객관적인 평가가 가능하다[18, 19].

23 NYCRR 500의 모의침투 테스트 및 취약성 평가는 위험평가에 기초하여 비공개 정보를 다루는 정보시스템에 대하여 이루어진다. 반면, 국내 금융기관들이 수행하는 취약점 분석 및 평가의 범위는 전자금융기반시설에 해당되는 계정계 시스템에 한하여 이루어지며, 대상은 총자산 2조 원 이상이고 상시 종업원 수가 300명 이상인 금융기관으로 높은 기준이 설정되어 있다. 이는 금융서비스 산업 전반이 아닌 특정 금융기관 및 업무의 사이버보안 수준을 높이는 데 집중하고 있다.

금융기관들이 감독기관에 제출하는 보고서는 금융서비스 산업의 사이버보안을 효과적으로 규제하고 감독하는 중요한 요건이며, 금융기관의 원활한 정보보안 거버넌스에 필수적이다. 이에 따라 보고 대상 금융기관의 기준을 낮추고 위험평가를 기반으로 실제 수행한 사이버보안 활동 보고서를 감독기관에 보고하도록 보고 의무를 강화해야 한다.

5.4 CISO 임명의 다양성 확대

23 NYCRR 500은 제3자 서비스 제공자도 CISO의 자격이 될 수 있도록 하여 금융기관의 자율성을 인정하였다. 이는 CISO의 전문성을 바탕으로 해당 금융기관에 맞는 창의적이고 혁신적인 사이버보안 시스템을 구축하도록 하는 취지를 반영한 것이다. 이와 달리 전자금융거래법은 사실상 내부 임직원(in-house)만 CISO 임명이 가능하며 사이버보안 전문가가 부족한 국내에서는 능력 있고 유능한 CISO를 채용한 몇몇 금융기관들만 사이버보안 수준이 높아지는 효과가 있다. 이에 사이버보안에 전문성을 가진 교육기관, 연구기관, 법무 법인, 컨설팅 법인 등 전자금융거래법에서 요구하고 있는 자격요건 이상을 갖춘 능력 있고 유능하며 검증된 제3자 서비스 제공자도 CISO 임명이 가능하도록 선택의 폭을 넓혀 특정 금융기관뿐만이 아닌 금융서비스 산업 전체의 사이버보안 수준을 높일 필요가 있다. 제3자 서비스 제공자가 CISO로 임명되더라도 사이버보안 업무의 독립성과 책임성을 강화하기 위하여 제정된 CISO의 겸직 금지 의무는 지속되어야 한다.

6. 결 론

본 논문은 금융 사이버보안 규제의 국제경쟁력 제고를 위한 방안으로 2017년 미국 뉴욕 주에서 시행된 23 NYCRR 500 금융 사이버보안 규정을 분석하여 국내 현행법 개선을 위한 대안을 제시하였다.

국내 금융기관의 해외진출 지원 및 해외 금융기관의 국내 유치 측면에서 사이버보안에 대한 국제적인 흐름을 준수할 수 있도록 국내 사이버보안 규정이 정비되어야 할 것이다. 그리하여야 국내·외에서 영업활동을 하고 있는 금융기관이 사이버보안 규제의 국제 수준에

합리적이고 탄력적으로 대응할 수 있을 뿐만 아니라 규제순응비용까지 경감할 수 있다. 23 NYCRR 500에서는 최소 기준 제시 및 전문기관에서 개발한 사이버보안 프레임워크에 기초하여 효과적인 금융 사이버보안 규제를 마련하였다. 우리나라 또한 사이버보안 사건이나 사고가 있을 때마다 금융 사이버보안 규제를 제·개정하는 기존의 방식에서 탈피하여 원칙중심의 일관성 있는 사이버보안 규제체계를 제시해야만 금융서비스 산업분야에서 국제적인 위상을 갖출 수 있게 될 것이다.

본 연구는 국내 금융 사이버보안의 제도·정책 개선 측면에 초점을 맞추고 있으며 금융 사이버보안 규제를 관리·감독하는 감독기관의 조직·인력시스템 개선에 대한 연구는 추후 과제로 이어져야 할 것이다.

References

[1] Dixon, H., “Maintaining Liability in AML and Cybersecurity at New York’s Financial Institutions,” Penn State Journal of Law & International Affairs, Vol. 5, No. 1, pp. 73-110, 2017.

[2] Do, H. J., “A Study on Cloud Computing for Financial Sector limited to Processing System of Non-Critical Information: Policy Suggestion based on US and UK’s approach,” The Journal of Society for e-Business Studies, Vol. 22, No. 4, pp 39-51, 2017.

[3] Drew, K., “NYCRR History and the Process of Keeping it Up to Date: Important Information for Using this Database,” Appellate Division 4th Dept. Law Library, Rochester, NY, 2014.

[4] Ernst & Young LLP, Cybersecurity requirements for financial services companies, https://www.ey.com/Publication/vwLUAssets/EY-cybersecurity-requirements-for-financial-services-companies/$FILE/EY-cybersecurity-requirements-for-financial-services-companies.pdf, Feb. 2017.

[5] Federal Financial Institutions Examination Council(FFIEC), About the, https://www.ffiec.gov/about.htm, Aug. 2018.

[6] Federal Financial Institutions Examination Council(FFIEC), Cybersecurity Assessment Tool, May 2017.

[7] Federal Financial Institutions Examination Council(FFIEC), Information Technology Examination Handbook: Information Security, Sep. 2016.

[8] Federal Trade Commission(FTC), Financial Institutions and Customer Information: Complying with the Safeguards Rule, Apr. 2006.

[9] Financial Services Committee(FSC), Plan to Expand Cloud System within Financial Institutions, Jul. 2018.

[10] Financial Services Committee(FSC), Summary of Global Financial Center Planning and Development 2017~2019 in Korea, Sep. 2017.

[11] Financial Supervisory Services(FSS),

Handbook for Regulation on Supervision of Electronic Financial Transactions, pp. 2-19, FSS, May. 2017.

[12] Hwang, I. H., Monetary Penalty is sweeping across NY, Alert for Korean Banks, MK News, http://news.mk.co.kr/newsRead.php?sc=30000001&year=2017&no=755334, Nov. 2017.

[13] IEEE Standards Association, GRAMM-LEACH-BLILEY ACT, http://grouper.ieee.org/groups/2600/presentations/Laws/GLBDoc.pdf, 2018.

[14] Kim, M., Mapping of NYDFS Cybersecurity Regulations to NAIC Insurance Data Security Model Law, Johnson Lambert, 2017.

[15] Kosseff, J., "New York's Financial Cybersecurity Regulation: Tough, Fair, and a National Model," Georgetown Law Technology Review, Vol. 1, No. 2, pp. 436-444, 2017.

[16] Michelle Misko, Choosing the Right Cybersecurity Assessment Tool, TraceSecurity, https://www.nascus.org/events/cyber2016/Misko.pdf, 2016.

[17] Mooney, J., Borden, R., and Jeanite, S., edgwick South Carolina's New Insurance Data Security Act: Pebbles Before a Landslide?, White and Williams LLP, 2018.

[18] New York State Department of Financial Services, 23 nycrr 500: Cybersecurity Requirements for Financial Services Companies, https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf, 2017.

[19] New York State Department of Financial Services, 23-NYCRR-500 DFS Cybersecurity Regulation, U.S. Department of the Treasury, 2017.

[20] New York State Department of Financial Services, History, https://www.dfs.ny.gov/about/history.htm, 2018.

[21] New York State Department of Financial Services, Who We Supervise, https://www.dfs.ny.gov/about/whowesupervise.htm, 2018.

[22] Park, W. I., "Protection of Personal Credit Information in the Cross-border Financial Transactions," Kyung-Hee University Law Journal, Vol. 41, No. 1, pp. 149-176, 2006.

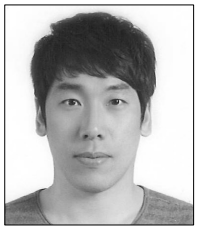
[23] Pruitt, J. S., Legal Alert: NY DFS Announces Proposal for Cybersecurity Rules for Financial Services Companies, Eversheds Sutherland (US) LLP, 2016.

[24] Thomson Reuter West Law, New York Codes, Rules and Regulations, https://govt.westlaw.com/nycrr/Index?transitionType=Default&contextData=(sc.Default), 2018.

[25] U.S. Government Publishing Office, Electronic Code of Federal Regulations, https://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=1e9a81d52a0904d70a046d0675d613b0&rgn=div5&view=text&node=16%3A1.0.1.3.38&idno=16, 2018.

[26] Yeandle, M., The Global Financial Centres Index 23, pp. 2-43, Z/Yen, 2018.

저 자 소 개



김도철 (E-mail: kimdo72@korea.ac.kr)
2015년～현재 고려대학교 정보보호대학원 금융보안학과 석사과정
2018년～현재 농협중앙회 농협미래경영연구소
관심분야 사이버보안 정책, 사이버보안 국제표준, 머신러닝, 데이터 마이닝

김인석 (E-mail: iskim11@korea.ac.kr)
2008년 고려대학교 정보경영공학대학원 (박사)
2009년～현재 고려대학교 정보보호대학원 교수
FDS산업포럼 회장, 한국정보보호학회 운영위원
관심분야 전자금융보안, 금융 IT 컴플라이언스, 핀테크