23 NYCRR 500

NYCRR 500 원문보기

CYBERSECURITY REQUIREMENTS FOR FINANCIAL SERVICES COMPANIES

美금융 데이터중심 보안 체계 강화

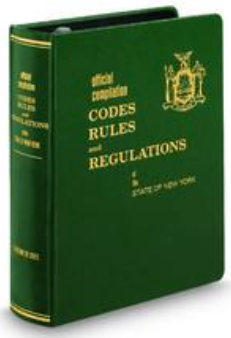
SOMANSA

개요

- 금융서비스업 규제인 Title 23 Financial Service의 NYCRR 500 은 뉴욕금융서비스국 (NY Department of Financial Services)장이 공포한 규정으로 2017년 3월 1일 시행, 뉴욕주의 모든 금융기관에 적용되는 사이버보안 규정

- 기존의 금융IT보안 규제와 달리 **데이터 중심 보안 체계구축을 위한 조항(유출통제, 파기, 접근통제, 암호화 등)**들이 포함되어있어 그동안 정보 보안 투자 대부분을 차지해 온 네트워크 보안과 달리 데이터 및 데이터가 포함된 정보시스템 보안을 강조

- 전세계 금융의 메카인 뉴욕에 적용,
  전세계 금융기관의 향후 보안 전략 수립에 새로운 영향을 끼칠것으로 예상



뉴욕 행정규정 NYCRR
(New York Codes, Rules and Regulations)

적용대상 및 시행일자

SOMANSA

적용대상

- 뉴욕 주 은행법과 보험법 또는 금융 서비스법에 의거해
  면허, 등록, 인가, 증명, 허가, 승인, 기타 유사한 허가를
  받아 사업을 운영하는 개인과 비정부 기관은 모두 적용 대상

시행일자

- 2017년 3월 시행

- 시행일로부터 180일의 유예기간
  (2017년 8월28일까지)

보호대상 데이터 및 조치의무

SOMANSA

- **Nonpublic Information (NPI): 비공개 정보**
  - 개인정보 (Personal Information) 보다 더 광범위

Non Public Information (NPI)의 정의
① 사업관련 정보 (유출 시 사업, 운영, 보안 등에 중대한 부작용을 초래하는 정보)
② 개인(고객)정보, 개인식별정보(PII), 금융정보, PW, 생체인증정보 등
③ 건강정보 (Healthcare-related)

- **NPI를 주기적으로 안전하게 파기 (500.13):**
  사업상에 필요한 기간이 지나거나, 법규정에 의해 보유하여야 하는 경우를 제외하고
  NPI는 주기적으로 안전하게 파기하여야 함

- **NPI 접근기록 무단조회, 유출통제 구축 (500.14):**
  인가된 사용자의 활동에 대한 모니터링 뿐만 아니라
  비인가자의 NPI 무단 접근을 탐지하기 위한 정책, 절차 수립, 통제 구축

- **보유 NPI 암호화, 전송 NPI 암호화, 불가한 경우 대체 방안 수립 (500.15):**
  보유 또는 전송하는 NPI의 보호를 위한 암호화 조치 필요
  외부 네트워크를 통해 전송 또는 보유대기중인 NPI의 암호화가 불가능할 경우 CISO 승인하에
  보호가능한 대체방안 수립이 가능

- **접근권한 통제 (500.07):**
  NPI에 접근가능한 정보시스템 접근권한을 설정하고 주기적으로 접근권한 검토

- **외부접근에 대한 인증방법 강화 (500.12):**
  NPI 또는 정보시스템에 비인가 접근 방지를 위해 다중요소 인증 또는 위험기반 인증 필요
  외부 네트워크에서 내부 네트워크로 접속하는 모든 사용자에는 다중요소 인증 필수

그외의 주요 보안요구사항

SOMANSA

- **제 3자 서비스 제공자(Third Party Service Provider) 관리 필수 (500.11):**
  제3자 서비스 제공자가 접근, 보유할 수 있는 정보시스템 및 NPI의 보안을 위해 정책 및 절차를 마련.
  여기에는 제3자 서비스 제공자 식별, 위험평가, 최소 보안요구사항 이행에 대한 내용과 NPI 및
  정보시스템 접속시 다중요소인증, 전송시 암호화, NPI 및 정보시스템에 영향을 줄수 있는 사건 보고
  등이 포함되어야 함

- **응용 프로그램 보안 (500.08):**
  사내에서 안전한 응용프로그램 개발을 위한 절차, 가이드라인, 표준 등을 마련.
  외부에서 개발된 응용프로그램에 대한 보안평가, 테스트 절차를 마련해야 함

- **위험평가 (500.05):**
  정보시스템에 대해 주기적으로 위험평가를 수행, 위험요소를 도출하고 이를 완화시킬수 있는 요구사항 마련

- **보안사고/이벤트 기록 유지 (500.06):**
  금융거래내역 최소 5년이상, 사이버 보안 사건(Event)은 최소 3년이상 보관,
  감사기록을 안전하게 보관할 수있는 시스템 필요

신용정보보호법과의 비교

SOMANSA

분류	항목	NYCRR 500	신용정보법
일반	적용시기	2017년 3월 시행	2016년 10월 개정(법) 시행
	적용대상	뉴욕주의 금융기관	대한민국내 신용정보를 이용·제공하는 금융기관, 신용정보회사, 신용정보집중기관
	보호대상 데이터	**NPI (비공개정보):** 개인정보 (PII, 바이오정보 포함), 금융정보, 사업기밀, 건강정보 등	신용정보, 개인신용정보 (개인정보 포함)
	주요특징	NPI 데이터 중심의 보호조치	기존 금융기관이 적용받던 개인정보보호법, 망법 등 유사규제를 신용정보법으로 일원화
		제3자 제공업체 관리감독 기준 강화	
		응용프로그램의 보호	형사처벌 및 징계에 대한 수위가 높음
		NPI 데이터 암호화 혹은 암호화에 준하는 보호조치 인정	
	위반시 징계	미국의 특성상 유출사고 발생시 집단소송으로 충분히 기관을 징계할 수 있기에, 과징금, 형사처벌등에 대한 규정이 없음	과태료, 과징금, 형사처벌, 업무정지 등
기술적 보호조치	데이터 보유제한	NPI 자산식별, 보유기간 통제, 파기 강제	신용정보 자산식별, 보유기간 통제, 파기
	데이터 암호화	NPI 저장 및 전송시 암호화 불가피할 경우에는 대체수단 강구	개인신용정보 암호화 보관, 전송시 암호화 송수신
	데이터 모니터링	NPI 접근통제, 과다조회 및 유출통제를 위한 모니터링 강화	개인신용정보 신용정보 유출통제, 과다조회 통제를 위한 모니터링 강화 (출력, 복사, 보조저장매체, 이메일 등)
	응용프로그램 보안	사내 개발, 외부 개발 응용프로그램에 대한 보호조치	상대적으로 강조가 덜되어있음
	인증	다중요소인증 등 강화된 인증 (외부에서 내부 접속시 필수)	(감독규정*) 중요 정보처리시스템 접근시 ID/PW 이외의 추가인증 (2-Factor)
	접근통제	NPI 접속시 접근통제 강화, 접근권한 주기적 검토	주요 데이터 접속시 접근통제 강화, 접근권한 최소화 및 주기적 검토

***신용정보법은 금융기관 대상으로 적용, 전자금융감독규정 또한 적용대상**

기술적 대응방안 총정리

SOMANSA

항목	기술적 보호조치	소만사 대응 솔루션
Data Asset Assessment (NPI 식별과 파기)	PC, DBMS, Server, Cloud 에서의 [NPI] 식별 및 보유기간 경과 데이터 파기	**Privacy-i, Server-i**
Access Control (NPI 접근통제)	[NPI] 접근통제, 과다조회 통제, 접속기록관리, 조회시스템	**DB-i, WAS-i, App-i**
Monitoring / DLP (NPI 유출통제)	[NPI] USB Copy, 출력, 인터넷, 웹메일, Monitoring 및 유출통제	**[Endpoint DLP] Privacy-i** **[Network DLP] Mail-i**
Encryption (NPI 암호화)	PC, DBMS, Server, Cloud 에서 [NPI] 식별 및 암호화	**Privacy-i, Server-i**
Authentication (NPI 접근시 인증)	(외부) Application 등을 통해 [NPI] 를 포함한 정보시스템 접속시 Multi-Factor 인증	

SOMANSA

500.02~500.17, 16항목 준수

Section	Title	
500.00~01	Introduction / Definition	서론 / 정의
500.02	CyberSecurity Program	사이버보안 프로그램
500.03	CyberSecurity Policy	사이버 보안 정책
500.04	Chief Information Security Officer (CISO)	정보보호책임자 임명
500.05	Penetration Testing and Vulnerability Assessment	모의침투 테스트 및 취약성평가
500.06	Audit Trail	감사추적
500.07	Access Privileges	접근권한
500.08	Application Security	응용프로그램 보안
500.09	Risk Assessment	위험평가
500.10	Cyber Security Personnel and Intelligence	사이버 보안요원 및 지능
500.11	Third party Service provider Security Policy	제3자 서비스 제공자 보안정책
500.12	Multi-Factor Authentication	다중요소 인증
500.13	Limitation on Data Retention	데이터 보유 제한
500.14	Training and Monitoring	교육과 모니터링
500.15	Encryption of Nonpublic Information	비공개 정보 암호화
500.16	Incident Response Plan	사고대응 계획
500.17	Notices to Superintendent	감독기관 보고
500.18~ 500.23	Confidentiality, Exemptions, Enforcement	기밀보장, 적용면제
	Effective Date, Transitional Period, Severability	시행일자, 유예기간 등

SOMANSA

500.02~500.17, 16항목 준수

Section	Title	요약
500.02	사이버보안 프로그램	위험평가(Risk Assessment)를 통해 해당 기관 정보시스템(IS)의 기밀성, 무결성, 가용성을 보장하는 보안프로그램 확립
500.03	사이버 보안 정책	기관이 보유하고 있는 비공개정보(NPI) 및 정보시스템 보호를 위한 정책 수립
500.04	정보보호책임자 임명 및 역할	사이버 보안 프로그램/정책을 주도할 자격을 갖춘 CISO 임명, 역할 이행
500.05	모의침투 테스트 및 취약성평가	위험평가에서 도출된 위험요소를 기반으로 연간 모의침투 테스트 실시, 2년마다 취약성평가 실시
500.06	감사추적	금융거래내역 최소 5년이상, 사이버 보안 사건(Event)은 최소 3년이상 보관
500.07	접근권한	NPI에 접근가능한 정보시스템 접근권한 설정, 주기적으로 접근권한 검토
500.08	응용프로그램 보안	사내에서 안전한 응용프로그램 개발을 위한 절차, 지침 등 마련, 보안평가 등
500.09	위험평가	절차에 따라 주기적 위험평가 수행 (NPI, 정보시스템 변경 시 등)
500.10	사이버 보안요원 및 지능	사이버 보안 위험에 대응할 수 있는 보안전문 인력 확보, 위험 대응 교육 제공
500.11	제3자 서비스 제공자 보안정책	제3자 서비스 제공자가 접근, 보유하고 있는 정보시스템 및 NPI의 보호를 위한 정책 및 절차 수립 (식별, 위험평가, NPI 전송 시 암호화 등)
500.12	다중요소 인증	NPI 또는 정보시스템 비인가접근 통제를 위한 다중요소/위험기반 인증 도입, 외부에서 내부 네트워크 접근시 필수 (CISO가 동등한 기술조치시 대체가능)
500.13	데이터 보유 제한	불필요한 NPI를 주기적으로 파기할 의무
500.14	교육과 모니터링	인가된 사용자 활동 감시 및 비인가자의 NPI 무단접근에 대한 내부통제 구축, 보안의식 제고를 위한 임직원 교육
500.15	비공개 정보 암호화	기관에서 보유 또는 전송하는 NPI에 대해 암호화 조치
500.16	침해사고대응 계획	침해사고에서 대응 및 신속한 복구를 위한 계획 수립
500.17	감독기관 보고	보안사건 발생시 72간 내 감독기관 신고, 규정 컴플라이언스 여부 연간보고