NIST의 사이버 보안 프레임워크 주요내용

< 목 차 >

1. 개요

▶ 미국 국립표준기술연구소(NIST)가 새로운 개인정보보호 프레임워크 개발을 위한 프로젝트를 시작한다고 발표 ('18.9.4.)

- NIST는 기업들이 위험을 관리 할 수 있도록 자발적 개인정보보호 프레임워크를 개발하기 위한 공동 프로젝트[382]를 추진
- NIST의 Walter G Copan 소장은 NIST가 사이버 보안 프레임워크(NIST Cybersecurity Framework)의 광범위한 채택을 통해 큰 성공을 거두었다며, 이는 개인정보 위험 관리를 위한 보완적인 지침을 제공하는 것으로 볼 수 있다고 언급
- NIST의 사이버 보안 프레임워크(NIST Cyber security-Framework)는 2014년 2월 12일 버전 1.0(Framework for Improving Critical Infrastructure Cybersecurity Version 1.0)이 공개되었으며, 2018년 4월 16일에는 개정판에 해당하는 「인프라 사이버 보안 개선을 위한 프레임워크 1.1(Framework for Improving Critical Infrastructure Cybersecurity Version 1.1)」 이 발표됨

382 이를 통해 개발될 개인정보보호 프레임워크는 기업/조직들이 유연하고 효과적인 개인정보보호 솔루션을 위한 전략적 우선순위를 정할 수 있도록 지원하고, 이를 통해 개인들이 신뢰를 바탕으로 혁신적인 기술의 이점을 누릴 수 있도록 하는 엔터프라이즈 차원의 접근 방식을 제공할 예정

2. 미국 NIST의 사이버 보안 프레임워크 추진 배경

▶ NIST의 사이버 보안 프레임워크는 국가 주요 기반시설의 사이버 보안 강화를 위해 추진되었으며, 트럼프 행정부 출범 후 연방정부 기관들의 보안 위협 점검을 위한 목적으로 확대

- 사이버보안 프레임워크 1.0은 2013년 2월 오바마(Obama) 대통령이 발표한 '국가 주요 기반시설의 사이버 위협 대응 강화를 위한 행정명령(Improving Critical Infrastructure Cybersecurity Executive Order 13636)'에 따라 마련
  - 동 프레임워크의 목적은 국가 주요 기반 시설 운영 주체가 사이버 위협 상황에 대한 인식 및 적절한 대응을 수행할 수 있도록 하는 것
- 2017년 5월 트럼프 미국 대통령이 발표한 '연방 네트워크 및 핵심 인프라의 사이버 보안 강화에 관한 행정 명령'에 따라 「인프라 사이버 보안 개선을 위한 프레임워크 1.1」을 준비[383]
  - 동 프레임워크는 에너지, 은행, 통신, 국방 산업 기지를 포함한 국가 주요 기반 시설의 운영 주체가 사이버 위협 상황에 대한 인식 및 적절한 대응을 할 수 있도록 안내하는 일종의 관리 가이드라인
- 동 행정명령과 관련해 NIST는 2017년 5월 12일 연방정부 기관들이 사이버보안 프레임워크를 도입하고 활용할 수 있는 방법에 대한 안내 자료(draft implementation guide)를 발표[384]
  - 가이드는 사이버보안 관련 책임에 대한 기관들의 대응 방법으로 △조직과 사이버보안 위험 관리를 통합할 것 △사이버보안 필요요건을 관리할 것 △사이버보안 및 구매 프로세스를 통합하고 일치시킬 것 △조직의 사이버보안을 평가할 것 △사이버보안 프로그램을 관리할 것 △사이버보안 위험에 대한 전반적인 이해를 유지할 것 △사이버보안 위험을 보고할 것 △맞춤화된 프로세스를 고지할 것 등 8가지를 제시

3. 사이버 보안 프레임워크 주요내용

▶ 사이버 보안 프레임워크 1.1은 사이버 보안 위험을 관리하기 위한 위험 기반 접근방식이며, △프레임워크 코어, △프레임워크 구현 계층 △프레임워크 프로파일 등 세 부분으로 구성[385]

- 첫째, 프레임워크 코어(The Framework Core)는 주요 인프라 분야에 공통되는 사이버 보안 활동,

383 NIST의 사이버보안 프레임워크는 원래 주요 기반시설 분야에 한정된 것이었으나, 트럼프 대통령은 연방정부 기관들로 하여금 NIST의 사이버보안 프레임워크에 따라 자체적인 보안위협을 점검하도록 행정명령
384 출처: https://gcn.com/articles/2017/05/16/nist-cybersecurity-framework.aspx
385 출처: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

기대되는 성과, 적용 가능한 참조 자료 등의 세트를 의미

- 주요 기반시설에 대한 사이버보안 대응 프로세스를 인지(Identify), 보호(Protect), 탐지(Detect), 대응(Respond), 복구(Recover)로 구분하고 각 활동을 정의

• 둘째, 프레임워크의 구현 계층(Framework Implementation Tiers)은 조직이 처한 위기관리 상황, 위협 환경, 법률 및 규제 요건, 사업 목적, 임무 우선순위, 예산 등에 따라 적용 가능한 단계별 사이버 보안 위험 관리 방식을 제시

- 각 단계는 △부분적 적용(Tier 1: Partial) 단계 △위험 정보 활용 단계(Tier 2: Risk-Informed) △위험 정보 활용 및 반복 단계(Tier 3: Risk-Informed and Repeatable) △적응 단계(Tier 4: Adaptive)로 구분

• 셋째, 프레임워크의 프로파일(Framework Profile)은 조직이 수행하고 있는 사이버 보안 활동의 현재 상태와 목표 상태의 격차를 파악하고 이를 최소화할 수 있는 해결 과제 도출 방안을 제시[386]

- 조직의 요구 사항, 위험 허용 한계치, 재원 등을 고려하여 '프레임워크 코어'가 제시한 프로세스별 달성 목표 수준 및 현재 상태를 작성하고, 양자를 비교하여 조직이 우선적으로 수행해야 할 사항이 반영된 로드맵을 수립

▶ 사이버 보안 프레임워크 버전 1.1은 2014년의 버전 1.0 발표 이후 이행된 표준의 개정내용을 포함

• 버전 1.1에서는 △사이버 보안 프레임워크 인증 및 신원 △사이버 보안 위험 자가 평가 △공급망 내의 사이버 보안 관리 △취약점 분석의 관한 업데이트가 포함됨

• 사이버 보안 위협의 자가 평가 부분을 추가하고 공급망 내의 사이버 보안 리스크 관리(Cyber Supply Chain Risk Management)를 위해 동 프레임워크를 활용하는 것에 대한 설명을 확대하는 등 새로운 내용을 추가

• '컴플라이언스'와 같이 혼란을 야기하거나 사이버 보안 프레임워크의 이해관계자들 사이에서 서로 다른 의미로 해석될 수 있는 용어들을 정비하고, 허가, 인증, 신원 증명 등에 대한 설명을 정교화

• '프레임워크의 구현 계층'과 '프레임워크의 프로파일' 사이의 관계에 대해 더 발전된 설명을 제공

▶ 사이버 보안 프레임워크 1.1 버전은 기존 프로세스를 대체하도록 설계되지 않았으며, 현행 프로세스를 사용하여 이를 프레임워크에 오버레이하는 방식으로 현재의 사이버 보안 위험 접근법의 간극을 판별하고 개선 로드맵을 개발할 수 있음을 강조하며 사이버 보안 프레임워크를 이용하는 6가지 방법을 제시[387]

386 '프레임워크 프로파일'에서는 프로파일 설정 메커니즘만을 제공하고 있으며, 프로파일 설정에 필요한 특정 양식 등은 각 조직이나 부문 별로 목적과 필요에 따라 설정하도록 요구

387 출처: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

- 첫째, 사이버 보안 실무에 대한 기본적인 검토를 위해 활용
- 둘째, 사이버 보안 프로그램의 수립 또는 개선을 위해 활용
- 셋째, 이해 관계자와의 사이버 보안 요구 사항 전달을 위해 활용
- 넷째, 구매 결정을 위해 활용
- 다섯째, 새롭거나 개정된 참고자료에 대한 기회를 파악하기 위해 활용
- 여섯째, 프라이버시와 시민의 자유를 보호하기 위한 방법론으로 활용

4. 향후계획

▶ NIST는 텍사스 오스틴에서 2018년 10월 16일 열리는 공개 워크숍을 통해 데이터 개인정보보호에 관해 이해 관계자들과의 논의를 진행할 계획[388]

- 동 워크숍은 △개인정보 위험을 관리하는 현재의 관행에 대한 정보와 △일반적인 사이버 보안 관행을 뛰어 넘는 방식으로 프라이버시 리스크를 관리하기 위한 도전과제 및 요구사항을 수집하기 위해 계획된 시리즈 중 첫 번째 사례로 준비
- NIST는 2019년까지 이러한 워크숍 및 기타 홍보 노력을 통해 이해 관계자로부터 최상의 아이디어를 수집하고, 이를 바탕으로 NIST의 프레임워크 도구가 다양한 조직에 유용하고 효과적인 것이 될 수 있도록 할 계획

Reference

1. ExecutiveGov, “NIST Unveils New Project to Advance Privacy Framework for Public Stakeholders”, 2018.9.5.
2. Health IT Security, “NIST Cybersecurity Framework To Get Privacy Framework Companion”, 2018.9.5
3 GCN, "What's next for NIST cybersecurity framework?", 2017.5.16
4. IAPP, “NIST launches privacy framework project”, 2018.9.5
5. NIST, “Department of Commerce Launches Collaborative Privacy Framework Effort”, 2018.9.4
6. NIST, "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1", 2018.4.16.

388 출처:
https://www.nist.gov/news-events/news/2018/09/department-commerce-launches-collaborative-privacy-framework-effort