Headline

망분리의 한계를 넘는 새로운 보안 패러다임: 국가 망 보안체계(N²SF) 도입과 시사점

관제사업그룹 관제사업 3 팀 고광진 팀장

■ 개요

2003 년 1 월 25 일 발생한 분산 서비스 거부(DDoS) 공격은 대한민국의 초고속 인터넷망을 마비시켜 국가 전체를 혼란에 빠드린 사건이었다. 이 사건이 발생하기 전까지 우리나라는 세계적인 초고속 인터넷 강국으로 평가받고 있었다. 빠른 인터넷 기술을 기반으로 1,000 만 명이 넘는 보급률이라는 인상적인 수치도 나왔지만, 화려한 타이틀과 통계 이면에 숨겨진 취약한 정보보호 수준은 '1.25 인터넷 대란'을 계기로 '모래 위의 성'에 불과했음이 드러났다.

이후 2006 년 국가사이버안전전략회의에서 국가기관의 업무망과 인터넷망을 분리하는 정책이 보고되었고, 국가정보원과 안전행정부(현 행정안전부), 한국정보화진흥원(NIA)이 역할을 분담해 '국가기관망분리 구축 가이드'를 배포함으로써 각 부처와 기관들이 참고하도록 했다.

망분리는 지난 18 년여 동안 업무망과 인터넷망을 분리해 사고 발생 시 피해를 최소화하는 국가 공공기관의 핵심 네트워크 보안 정책으로 자리잡아 왔다. 이는 내부 자산을 보호하기 위한 최적의 보안 모델로 기능해왔으나, 경계망 기반의 구조로 인해 보안 영역과 비보안 영역을 평면적으로만 분리하는 한계가 있었다. 구조가 단순하다는 장점이 있는 반면, 물리적 또는 논리적으로 망을 분리함에 따라 고비용, 낮은 유연성, 불편한 사용성 등의 단점도 존재했다.

국가정보원은 이러한 IT 환경의 변화와 현장 애로사항을 반영해 망분리 정책을 시대 상황에 맞게 지속적으로 보완해왔다. 그러나 코로나 19 이후 원격근무, 클라우드, 생성형 AI 등으로 대표되는 IT 환경의 급격한 변화는 기존 망분리 환경에서는 효율적인 업무 수행을 어렵게 만들었다. 이에, 기존 망분리 정책의 한계를 보완하고 변화하는 기술과 환경, 위협에 유연하게 대응할 수 있도록 『국가 망 보안정책 개선 합동 TF』가 구성됐으며, 국가정보원은 이 TF 와 함께 보안통제를 업무의 중요도에 따라 차등 적용하는 '국가 망 보안 체계(National Network Security Framework, N²SF)'를 수립했다.

본 리포트에서는 국가 망 보안체계(N²SF)의 추진 목표, 적용 절차, 등급 분류, 보안 대책 등에 대해 자세히 살펴본다.

■ 국가 망 보안체계(N²SF) 추진 목표

국가정보원이 추진한 망분리 정책 개선 다섯 가지를 살표보면 아래와 같다.

첫째, 획일적인 망분리에서 탈피하여 국가 망 보안체계(N²SF) 기반으로 보안 정책의 패러다임을 전환한다.

둘째, 제약 없는 정보유통으로 신기술 융합을 강화하고 스마트 업무 환경을 조성한다.

셋째, 산·학·연·관 전문가와 함께 국내 실정에 최적화된 정책을 개발한다.

넷째, 새로운 보안 정책으로 공표함으로써 각급 기관의 제반 여건을 고려하면서 자율적으로 추진하되, 제도는 점진적으로 변화함으로써 안정적으로 정책이 안착되도록 한다.

다섯째, 공공 정보의 보안성과 활용성을 높이는 것과 함께 보안 기술 및 AI·데이터 산업 등 다양한 산업 발전· 육성으로 디지털 경제 창출에도 기여한다.

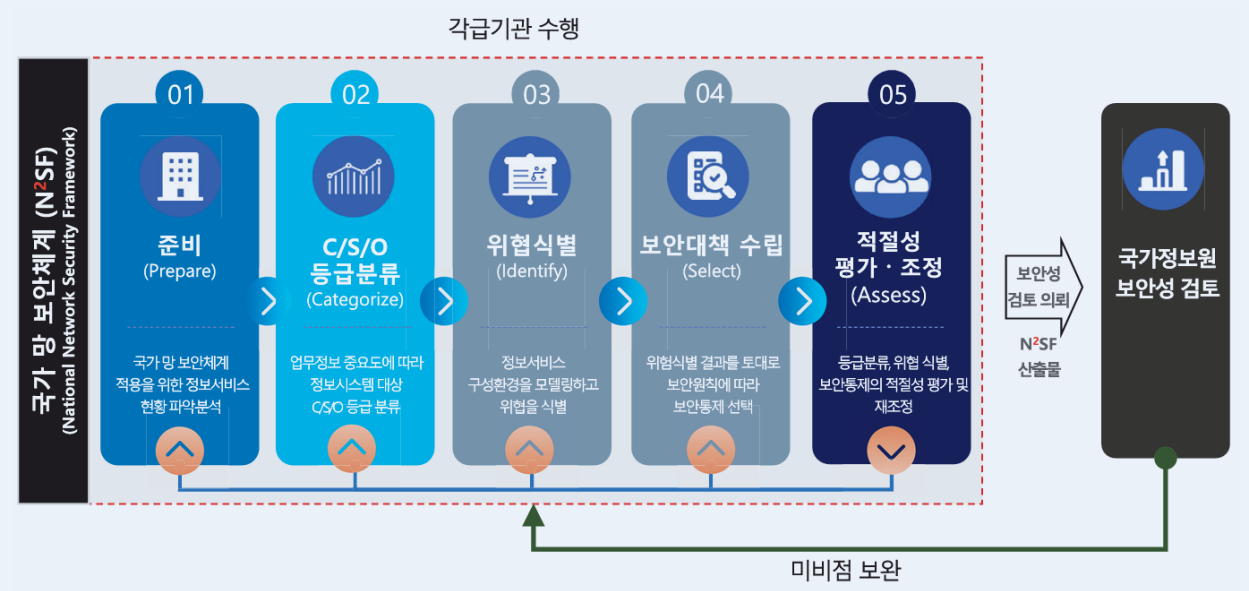
* 출처: 2024 정보보호 공시 현황 분석 보고서

그림 1. 망분리 정책 개선 추진 목표

또한, 국가 망 보안체계는 국가·공공기관의 업무 정보와 정보 시스템을 대상으로 법령 근거(정보공개법, 공공데이터법)에 따라 기밀(Classified), 민감(Sensitive), 공개(Open) 3 개 등급으로 분류하고, 등급별로 차등적인 보안통제를 적용하여 ①보안성 확보와 ②원활한 데이터 공유라는 두 가지 목적을 달성하는 정책이다.

■ 국가 망 보안체계(N²SF) 적용 절차

N²SF(국가 망 보안체계)는 총 5 단계의 절차로 구성된다. 이는 국가 및 공공기관이 정보화 사업을 계획하고 시행할 때, 해당 사업에 포함된 정보서비스에서 발생할 수 있는 보안 위협을 사전에 식별하고 위험 수준을 평가한 후, 이에 적절한 보안 대책을 수립하는 일련의 과정을 포괄한다. 각 단계에서 산출되는 결과물은 국가정보보안 기본지침에 따라 국가정보원의 보안성 검토 시 제출해야 한다.



* 출처: 2024 정보보호 공시 현황 분석 보고서

그림 2. 국가 망 보안체계 적용 절차

① 준비(Prepare) 단계에서는 기관의 업무정보 및 정보서비스 현황을 식별하고 분석하여, 이후 단계 수행에 필요한 기초적인 정보를 확보한다. 이를 바탕으로 국가 망 보안체계(N²SF) 적용 계획을 수립한다.

② C/S/O 등급 분류(Categorize) 단계에서는 기관의 업무정보 및 정보시스템의 중요도를 기준으로 C(Classified:기밀), S(Sensitive:민감), O(Open:공개) 등 3 단계로 등급을 분류한다.

③ 위협식별(Identify) 단계에서는 정보시스템을 포함한 서비스 환경 전체를 대상으로 한 모델링 기법을 활용해 위협을 식별하고, 보안 대책 적용이 필요한 대상을 선정한다.

④ 보안대책 수립(Select) 단계에서는 위협식별 결과를 기준으로 필요한 보안통제를 선택하고 구현계획을 수립한다.

⑤ 적절성 평가·조정(Assess) 단계에서는 준비 단계부터 보안 대책 수립 단계까지의 전 과정을 대상으로 적절성을 평가하고, 재조정·승인을 수행한다.

이처럼 국가 망 보안체계(N²SF)는 국가 및 공공기관이 자산(업무정보·정보시스템·정보서비스)을 분석해 위협을 식별하고 적절한 보안대책을 수립하도록 절차가 구성되어 있다.

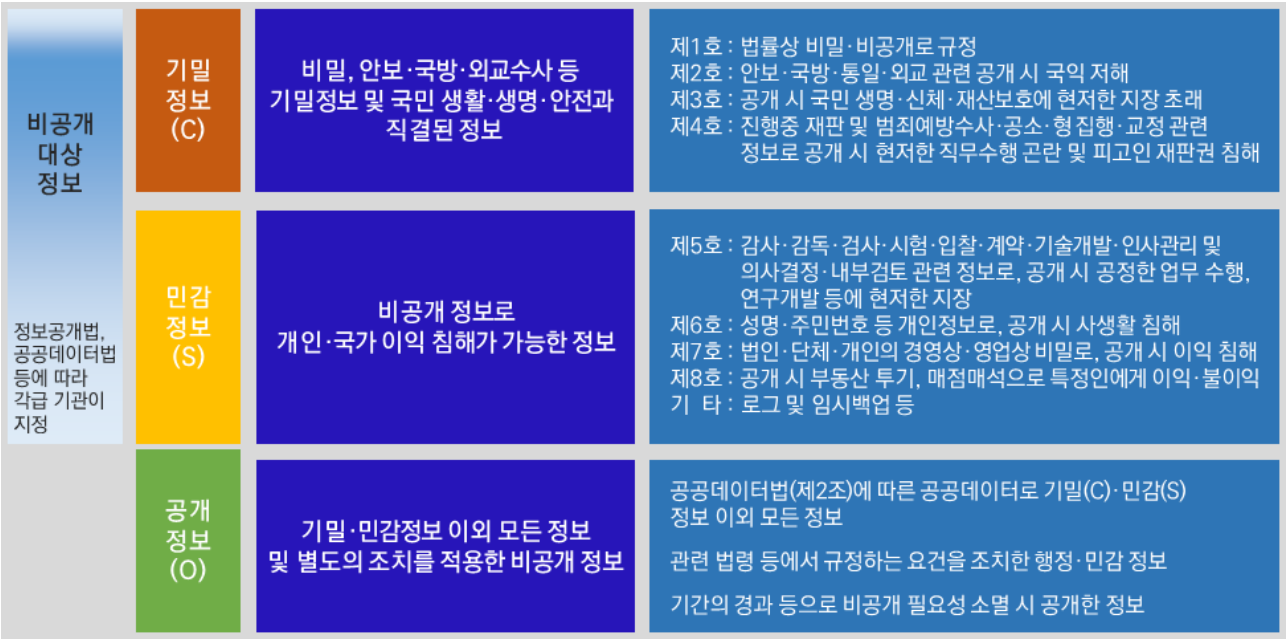
■ 국가 망 보안체계(N²SF) 등급 분류

국가 망 보안체계(N²SF)는 업무 정보와 정보시스템에 대해 각각 C/S/O 로 등급을 분류할 수 있으며, 분류의 기준은 관련법령의 근거에 따라 이루어진다.

기밀정보(Classified)는 비밀, 안보·국방·외교·수사 등의 기밀정보와 국민 생활·생명·안전과 직결된 정보로서 정보공개법 제 9 조(비공개 대상 정보)의 제 1 호부터 제 4 호까지를 포함한다.

민감정보(Sensitive)는 비공개 정보 등 개인·국가의 이익 침해가 가능한 정보로서 정보공개법 제 9 조(비공개 대상 정보)의 제 5 호부터 제 8 호까지의 정보 및 로그, 임시 백업 등의 기타 정보를 포함한다.

공개정보(Open)는 기밀정보(C) 및 민감정보(S) 이외의 모든 정보를 포함한다. 또한, 관련 법령 등에서 규정하는 요건을 조치한 비공개 정보를 포함해 기간의 경과 등 비공개 필요성이 소멸된 정보를 공개정보(O)로 분류한다.



* 출처 : 공공데이터법 및 정보공개법 참조

그림 3. 업무정보에 대한 C/S/O 분류 기준

■ 국가 망 보안체계(N²SF) 보안대책 수립

국가 망 보안체계(N²SF)는 정보서비스 모델링 단계에서 식별된 위협요소와 보안대책 적용지점에 관한 정보를 토대로 실시된다. 각 업무정보·정보시스템에 대한 보안통제 항목을 선택·조정한 후, 보안통제 구현계획을 수립해야 한다.

* 출처 : 국가 망 보안체계 보안 가이드 라인(Draft)

그림 4. 보안대책 수립 단계의 주요활동 연계도

또한, 보안대책 수립 단계의 주요 활동 및 산출물은 업무정보와 정보시스템에 대한 보안통제 항목에서 참고할 수 있다.

이처럼 N²SF의 준비단계부터 적절성 평가단계까지의 각 단계로 데이터 보안성과 활용성을 실현하는 것은 물론 공공기관의 업무 효율성을 높일 수 있게 됐다. 특히, 데이터 공유와 협업이 필요한 환경에서 효율성이 극대화될 것이다.

■ 주요국가 보안정책 동향

2014년 영국 정부가 수립한 GSCP(Government Security Classifications Policy, 정부 보안분류 정책)는 정보를 OFFICAL, SECRET, TOP SECRET 세가지 등급으로 분류한다. 각 등급은 정보 노출 시 국가안보, 경제적 이익, 국제 관계에 미칠 수 있는 피해의 심각성에 따라 결정한다.

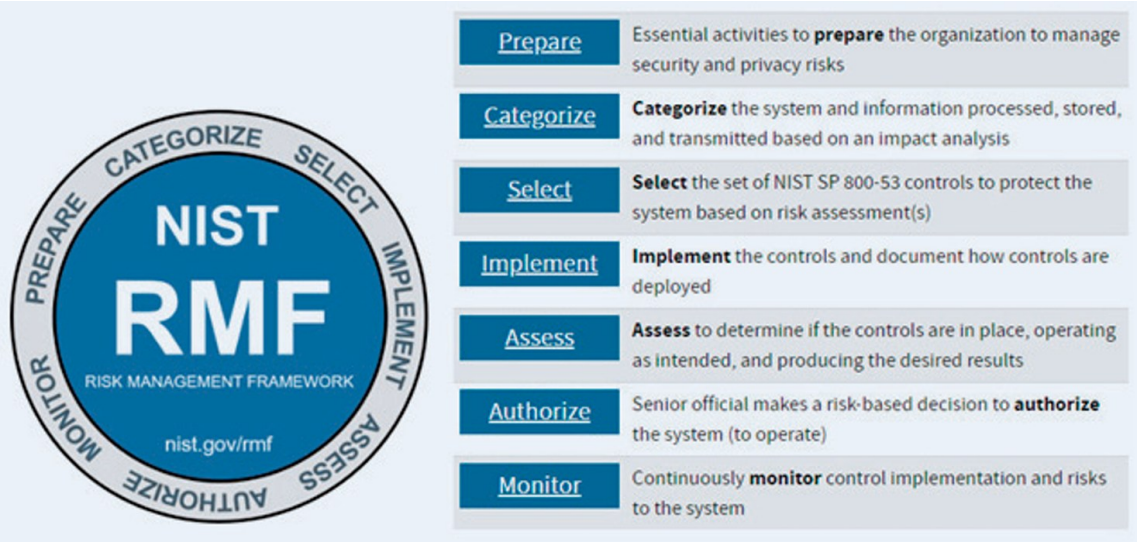
분류	정의 (정보 노출 시 파급력 수준)	보안 요구사항(개요)
TOP SECRET	국가안보와 직결되는 극도로 민감한 정보 (국가안보에 직접적이고 치명적인 피해)	적성국 국가배후 해킹조직 수준의 공격에 대한 보호
SECRET	고도의 보호가 필요한 민감한 정보 (국가의 안전과 운영에 심각한 피해)	국가배후 해킹조직, 고도화된 범죄조직 수준의 공격에 대한 보호
OFFICIAL	생산, 처리, 송수신되는 대부분의 공공정보 (피해가 없거나 미약한 피해)	내부자위협, 핵티비즘, 압력단체, 범죄조직 수준의 공격에 대한 보호

* 출처 : 영국정부 웹사이트 gov.uk

그림 5. 영국 GSCP(정부 보안분류 정책)

N²SF 역시 업무정보와 정보시스템을 기밀, 민감, 공개 등급으로 분류하는 등 관리하는 측면에서 GSCP와 매우 유사하다고 볼 수 있다.

미국의 NIST RMF는 미국 연방정보보안현대화법(FISMA)의 요구사항을 충족하는 모든 조직이 정보보안 및 개인정보보호에서의 위험을 관리하는데 사용하는 포괄적이고 유연한 위험관리 프레임워크다. NIST RMF는 7단계 절차로 구성되며 지속적인 보안강화를 위해 순화되는 개념을 담고 있다. 현재는 미국뿐만 아니라 캐나다, 호주, 뉴질랜드, 대한민국 등 많은 국가들이 이를 기반으로 한 자국의 위험관리 프레임워크를 개발하는 등 정보보안에 관한 위험관리 지침 및 표준으로 삼고 있다.



* 출처 : NIST CSRC

그림 6. NIST RMF 개요

캐나다 정부는 ITSG-33를 통해 자국의 정보보안 위험관리 프레임워크를 제공한다. ITSG-33은 NIST RMF를 바탕으로 캐나다 정부의 특정 요구사항을 반영해 개발되었다. 2009년 캐나다 정부의 보안정책에 따라 2010년 위험관리 프레임워크의 기본 틀을 개발하였고, 이후 2012년 프레임워크를 구체화한 기본 가이드라인을 발표했다.

년도	구분	관련문서 (지침, 가이드라인)	주요내용
2009	캐나다 정부 보안정책 수립	Policy on Government Security	
2010	위험관리 프레임워크	Framework for the Management of Risk	위험관리 개요 및 원칙
2012	가이드라인	ITSG-33 부록1	부서별 IT 보안 위험관리 활동
		ITSG-33 부록2	정보시스템 보안 위험관리 활동
		ITSG-33 부록3	보안통제 카탈로그
		ITSG-33 부록4	보안통제 프로파일
		ITSG-33 부록5	용어집

* 출처 : Canadian Centre for Cyber Security

그림 7. 캐나다 ITSG-33 연혁

ITSG-33은 위험관리 활동을 크게 부서별 IT보안 위험관리 계층과 정보시스템 보안 위험관리 계층으로 나누고, 두 개의 상·하위 계층을 유기적으로 연계할 수 있도록 했다.

ITSG-33의 보안통제는 NIST RMF의 보안통제를 기반으로 하기 때문에 보안통제 패밀리를 기술, 운영, 관리 등 3개의 클래스로 분류하고 있는 것이 특징이다. 각각의 클래스는 보안 매커니즘, 운영 절차, 관리 활동에 관한 보안통제를 포함하고 있다.

호주 정부의 ISM(Information Security Manual, 정보보안 매뉴얼)은 ISMS 를 기반으로 정부 기관의 정보보안 가이드라인을 제공하며 거버넌스, 식별, 보호, 탐지, 대응의 영역으로 구성된다. 호주 사이버보안센터는 사이버보안 사고감소 전략의 일환으로 사이버공격으로부터 네트워크를 보호하기 위해 실행해야 할 8 가지 기본적인 보안조치를 명시했다. 이 8 가지 기본 보안조치는 주로 예방적인 조치를 강조하며, 비교적 간단하게 측정하고 구현할 수 있도록 구성했다.

* 출처 : 호주 사이버보안센터

그림 8. 호주 ACSC 의 Essential Eight 의 보안통제 영역

국내에서는 국가·공공기관을 대상으로 국가 망 보안체계(N²SF)를 확산하려는 움직임이 보이고 있다. 이런 흐름에 대응하기 위해 여러 솔루션 업체들이 관련된 제품을 발빠르게 내놓고 있다. 국가정보원은 지난 18년간 국가·공공기관을 대상으로 추진하였던 망분리 환경을 완화하면서 보안은 강화시켰다. 새로운 방안으로 제시되고 있는 N²SF를 통해, 신기술 도입과 데이터 활용을 촉진하며 국가 사이버 보안 방어에 기여할 것으로 보고있다.

■ 국가 망 보안체계(N²SF) 관련 주요 가이드라인

국가 망 보안체계(N²SF)의 실질적 보안요소는 NIST-800-207(Zero Trust Architecture), NIST-800-53(Cyber Security Framework), MITRE ATT&CK V14,15를 참고해 만들어졌다. 다만, N²SF의 모태가 되는 ZTA는 국가·공공기관 보다는 기업을 고려해 만들어진 만큼 국가·공공기관이 실질적인 환경과 위협에서 대응이 어려울 것으로 판단해, 국가정보원에서는 ZTA와 ZTMM의 오버레이를 통해 자연스럽게 신기술이 적용되도록 N²SF를 만들었다. 올해 국정원에서 배포된 가이드라인과 해설서는 Draft 버전으로 금년 3분기에 정식 버전이 배포될 전망될 것으로 예상된다.

1. NIST, SP 800-207, ZTA

NIST(National Institute of Standards and Technology)는 미국 상무부 산하의 정부 기관으로, 다양한 기술 분야에서 표준과 모범 사례를 개발하는데 중요한 역할을 하고 있다. 특히 사이버 보안 분야에서 NIST는 정보 시스템 보안을 위한 권장 사항과 지침을 제공하는 800 시리즈로 전 세계에 널리 알려져 있다.

이 중 2020년 8월에 발표된 NIST SP 800-207은 제로트러스트 아키텍처(ZTA)에 대한 구체적인 가이드라인을 제공하는 문서로, 조직이 제로트러스트 모델을 도입하고 운영하도록 가이드라인을 제시한다. 해당 가이드라인은 제로트러스트 아키텍처에 대해서 정의한 최초의 표준 문서다. 이 후 발간된 가이드라인들은 NIST 800-207에서 정의한 제로트러스트 개념과 원칙을 참고하여 작성되었다.

2. NIST, SP 800-53

NIST, SP 800-53 (Cyber Security Framework)은 미국 상무부 산하 국립표준기술연구소(NIST)에서 개발한 정보보안 표준으로, 정보 시스템의 보안 및 개인정보 보호를 위한 통제(controls) 카탈로그를 제공한다.

미국 연방 정부 기관(국가안보 관련 기관 제외)을 대상으로 시행했으나, 5차 개정 이후로는 공공 및 민간 조직 모두가 사용할 수 있도록 변경돼 국제적으로 인정받는 사이버보안 프레임워크로 자리잡았다.

주요 특징은 정보시스템의 기밀성, 무결성, 가용성 보호와 위험 기반 접근법을 통해 보안 통제의 기준선을 선정하고 조직환경에 맞춰 조정할 수 있다는 점이다.

3. MITRE ATT&CK V14, 15

MITRE ATT&CK 프레임워크는 사이버 공격자의 전술(Tactics), 기술(Techniques), 절차(Procedures)를 체계화한 지식 베이스로, 보안 전문가들이 위협을 탐지하고 대응하는데 활용된다. 최신 버전인 v14와 v15에는 탐지 기능 강화와 새로운 공격 패턴이 반영됐다.

v14 주요 업데이트 내용은 ①측면 이동, ②ICS 자산 추가, ③모바일 위협 대응 확장, ④탐지 노트 개선 등이 있다. v15 주요 업데이트 내용은 ①분석 형식 개편, ②토큰 보호 완화 조치, ③크로스 도메인 통찰력, ④클라우드 매트릭스 강화 등이 있다.

두 버전 모두 실제 공격 사례를 반영한 지속적인 진화가 특징이며, 특히 v15에는 토큰 기반 공격 방어와 크로스 도메인 분석 기능에서 기술적 도약을 했다. 각 기관의 보안을 담당하는 조직은 이러한 업데이트 내용을 활용해 공격 수명 주기 전반에 걸친 예방·탐지·대응 전략을 수립할 수 있다.

결과적으로 국가 망 보안체계(N²SF)는 선택이 아닌 필수가 돼야 한다. 다만, 아직까지 시행한 사례가 없기 때문에 국가·공공기관에서 국가 망 보안체계(N²SF) 도입에 대해 의문이 많은 것은 사실이다. 국가정보원은 국가·공공기관이 국가 망 보안체계(N²SF)를 보다 쉽게 도입하고 운영할 수 있도록 필요한 ①가이드라인과 ②통제항목, ③정보서비스 해설서를 제공하고 있다. 다음 장에서는 국가 망 보안체계(N²SF) 주요 통제 항목에 대해서 알아보도록 하겠다.

■ 국가 망 보안체계(N²SF) 통제 항목

국가 망 보안체계(N²SF)는 업무 정보, 정보시스템을 대상으로 정보공개법과 공공데이터법에 따라 등급을 분류하여 위협을 도출하고, 통제 항목을 통해 보호 대책을 수립한다. 또한, 국가 망 보안체계(N²SF)에서 제공되는 통제 항목은 6개분야 약 180여개 항목으로 구성되어 있다. 각 기관은 이 통제 항목을 선별적으로 적용하여 유연성 있게 보호 대책을 수립하면 된다.

따라서 통제 항목 별로 요구되는 보안 조치와 이를 지원하는 주요 시스템(솔루션)은 N²SF 를 성공적으로 구현하기 위한 핵심 요소가 된다. 아래 주요 통제 항목을 간략하게 설명하고자 한다.

1. 권한

시스템 및 정보 접근 권한을 최소화하고, 철저한 신원 검증을 통해 인증된 사용자만 접근할 수 있도록 한다. 최소 권한 원칙을 적용해 불필요한 접근을 차단한다.

1-1. 최소권한(Least Privilege, LP)

최소권한은 사용자나 프로세스가 특정 업무를 수행하는 데 필요한 최소한의 권한만을 부여하는 보안 원칙으로 내부 및 외부 위협으로부터 보호하고, 내부 정보로의 불필요한 접근을 방지하기 위한 통제항목이다. 제한하는 방식으로 운영되는 이 권한의 식별자 필러에 연관된 주요 시스템은 아래와 같다.

1-2. 신원검증(Identity Verification, IV)

신원증명은 시스템 접근을 위한 자격 증명을 설정할 목적으로 대상 사용자의 신원 정보를 수집, 검증 및 확인하기 위한 통제항목이다.

1-3. 식별자관리(Identifier Management, IM)

식별자관리는 기관의 IT자산 및 인적 자원을 식별할 수 있는 고유한 식별자를 생성, 관리하여 접근 통제를 강화하고 인증 프로세스를 지원하기 위한 통제항목이다.

1-4. 계정관리(Account Management, AC)

계정관리는 시스템 내에서 사용자와 관련된 계정을 생성, 관리, 모니터링, 비활성화 및 삭제 기능을 수행하여 불필요한 계정 사용을 방지하고, 비 인가된 사용자 접근을 통제하여 보안성을 유지하기 위한 통제항목이다.

2. 인증

다중요소 인증(MFA)과 외부 인증수단 연계 등 다양한 인증 방식을 도입해 보안성과 편의성을 강화한다. 이를 통해 비인가자의 접근을 효과적으로 방지한다.

2-1. 다중요소 인증(Mutl-Factor Authentication, MA)

다중요소 인증은 기관 내부 사용자의 정보시스템 등에 접근 시 사용자 인증을 위해 두 개 이상의 인증 요소를 사용하여 보안성을 강화하기 위한 통제항목이다.

2-2. 외부 연계(External Integration, EI)

외부 연계 인증은 외부 기관 사용자에 대한 접근 시스템을 식별하고 시스템에 대한 접근 권한을 부여하기 위한 통제항목이다.

2-3. 식별(Identification, ID)

식별은 기관 정보시스템 및 시스템 구성장비에 대한 비인가 단말의 접속을 차단하기 위한 통제항목이다.

2-4. 인증보호(Authentication Protection, AU)

인증보호는 계정 인증 보안 강화 및 불법적인 계정 로그인 시도 방지, 생체 인증 공격 방지, 대체 보안수단 강구 등 인증 과정에서의 보안성 강화 및 다양한 위협에 대응하기 위한 통제항목이다.

2-5. 인증정책(Authentication Policy, AP)

인증정책은 기관 사용자 증명, 인증 프로파일, 그룹계정 사용자 인증 등 기관 내 사용자의 신원을 지속적으로 확인하고 보호하기 위한 통제항목이다.

2-6. 인증수단(Authentication Method, AM)

인증수단은 시스템 접근에 사용되는 인증의 생성, 변경, 보호, 갱신 등을 관리하기 위한 통제항목이다.

2-7. 로그인 (Login, LI)

로그인은 인증 피드백 보호, 로그인 시도 제한, 시스템 사용 알림, 인증 결과 처리 등 사용자 계정 인증 과정에서의 보안 위협 방지를 위한 통제항목이다.

3. 분리 및 격리

하드웨어와 소프트웨어를 활용한 물리적·논리적망분리 및 접근통제 기술을 적용한다. 필요 시 외부 연결을 제한하여 보안을 유지한다

3-1. 분리(Segregation, SG)

정보서비스 및 업무정보가 보안 등급에 따라 서로 다른 보안 도메인으로 구분되도록 하드웨어, 소프트웨어, 운영체제 분리 또는 인프라, 사용자 기능 분리를 통해 각 영역에 대한 보안을 강화하기 위한 통제항목이다.

3-2. 격리(Isolation, IS)

정보시스템은 각 프로세스를 독립된 공간에서 실행하여 상호 간섭을 차단하고, 일반 사용자에게 관리 기능 및 인터페이스의 노출을 제한하며, 애플리케이션 접근을 통제하여 데이터의 무단 접근을 방지하기 위한 통제항목이다.

4. 통제

데이터 전송 방식 및 유형을 통제해 중요 정보의 유출을 방지한다. 데이터 이동 경로와 전송 방법을 엄격히 관리한다.

4-1. 정보흐름(Information Flow, IF)

정보시스템 간에 정보가 이동할 수 있는 경로에 대한 관리 제어를 통해 비정상 동작, 외부 공격, 암호화된 정보의 흐름, 일방향 데이터 전송 및 차단, 메타데이터 활용, 정보전송 방식 제한, 보안 및 프라이버시 규칙 등을 통제하여 민감한 정보의 유출을 방지하고 안전한 정보흐름을 보장하기 위한 통제항목이다.

4-2. 외부경계(External Boundary, EX)

정보시스템 경계에서는 외부 네트워크와의 연결 접점을 제한하고, 승인된 통신만 허용할 수 있도록 경계 보호 장치를 활용하여 트래픽을 필터링하며, 이를 통해 외부로부터의 무단 접근을 차단하고 내부 정보시스템 구성요소 및 데이터 유출 방지, 개인 식별 정보에 대한 보호조치를 위한 통제항목이다.

4-3. 원격접속(Remote Access, RA)

원격접속 환경에서의 기밀성과 무결성 강화를 위한 접속 통제 및 통신구간 암호화, 관리자·사용자의 접속 위치 및 권한 사용에 대한, 무단 정보 유출 방지 및 일정 시간 이후 세션 자동 종료와 같은 안전한 원격접속을 위한 통제항목이다.

4-4. 세션(Session, SN)

세션 관리 및 보안은 각 세션의 고유 식별자를 할당하여 비정상 종료나 비활성 상태 시 즉시 종료하고 사용자의 요청 또는 조건에 따라 동시 세션 수 제한 자동 세션 종료, 알람 메시지 제공 등 세션의 보안통제를 통해 비인가 사용자 무단 접근과 정보 유출을 방지하기 위한 통제항목이다.

4-5. 무선망 접속(Wireless Network Access, WA)

무선 통신망 보안은 사용자 및 기기 인증, 통신 구간 암호화, 송수신 출력 제어, 승인되지 않은 무선망 차단, 그리고 외부인 전용 무선망 분리 및 무선망 관리 기능 보호를 통해 무선망의 기밀성과 무결성을 유지하는 통제항목이다.

4-6. 블루투스 연결(Bluetooth Connection, BC)

정보시스템에서 블루투스 사용 시 키보드, 마우스와 같이 사용자 입력을 위한 HID(Human Interface Device) 프로파일과 데이터 전송을 위한 FTP(File Transfer Profile) 기반의 통신을 구분하여 정보유출 위협이 발생할 수 있는 데이터 통신을 제한하는 통제항목이다.

5. 데이터

저장 및 전송 과정에서 암호화 기술과 키 관리 시스템을 적용해 데이터 보호 수준을 향상시킨다. 데이터의 안전한 저장과 처리를 보장한다.

5-1. 암호 키 관리(Encrytion Key Management, EK)

암호 키 관리는 암호 키의 생성, 배포, 저장, 사용 및 폐기 등 키의 전체 수명 주기를 안전하게 관리 하기 위한 프로세스로 키의 무단 접근과 오용을 방지하고, 데이터 기밀성과 무결성을 유지하기 위한 통제항목이다.

5-2. 암호기술 적용(Encrytion Technology Application, EA)

암호기술을 사용할 경우 보안등급과 용도에 따라 국가정보원장이 인증한 검증필 암호모듈 및 국가용 암호자재·장비를 사용하거나 특수목적용 암호자재·장비의 선택적 사용에 대한 통제항목이다.

5-3. 데이터 전송(Data Transmission, DT)

데이터 전송은 시스템 간 데이터 및 정보를 안전하게 전송하기 위한 보안 요구사항을 명확히 하고, 이를 관리하는 절차를 포함한다. 전송 중인 정보가 허가되지 않은 사람이나 시스템에 의해 읽히거나 변경, 손상되지 않도록 전송 기밀성과 전송 무결성을 보호하기 위한 통제항목이다.

5-4. 데이터 사용(Data Usage, DU)

데이터 사용은 검색, 연산 또는 기타 데이터 처리 활동과 같이 데이터가 정보시스템 내부에서 사용되는 동안에도 데이터에 대한 보호조치를 구현하는 통제항목이다.

6. 정보자산

모바일 기기, 하드웨어, 정보시스템 등 정보자산에 대한 보호 방안을 마련하고, 최신 기술을 반영해 지속적으로 관리한다.

6-1. 모바일 단말(Mobile Device, MD)

모바일 단말은 시스템에서 허용 및 금지할 모바일 코드와 모바일 코드 기술을 정의하고 허용할 모바일 코드와 모바일 코드 기술의 사용 제한 사항과 구현 가이드를 수립하여 내부 혹은 외부에서 모바일 단말의 사용 인가, 모니터링을 위한 통제항목이다.

6-2. 하드웨어(Device, DV)

하드웨어 보안 항목은 정보시스템과 하드웨어의 무결성을 유지하기 위해 펌웨어 및 하드웨어 구성 요소 검증, 그리고 실행 환경의 무결성 보장을 위한 통제항목이다.

6-3. 정보시스템 구성요소(Information System Component, IN)

정보시스템의 구성요소는 중앙화된 저장소를 통해 목록화하고, 설치·제거·업데이트 시 이를 정기적으로 갱신, 자동화된 매커니즘으로 최신성, 완전성, 정확성을 유지하여 불필요한 기능, 포트, 프로토콜, 소프트웨어를 비활성화 또는 제거하기 위한 통제항목이다.

위에서 간략하게 살펴본 봐와 같이 국가 망 보안체계(N²SF)의 보안통제 항목은 6개 영역의 180여개 항목으로 구성이 되어 있고, 현재 공식적으로 배포된 자료는 Draft버전으로 지속적으로 최신 기술과 기관·기업들의 목소리를 반영할 예정이다.

국가·공공기관에서 국가 망 보안체계(N²SF) 환경을 구현하기 위해서는 권한, 인증, 분리 및 격리, 통제, 데이터, 정보자산 등 통제항목에 대해 다양한 보안대책 작업들이 필요하다. 이러한 보안통제 항목을 업무정보와 정보시스템에 적용시켜 실시간으로 위협을 탐지하며, 동적 정책을 생성함으로써 조직의 보안 운영을 효율화하고 인적 자원의 부담과 보안 사고에 대한 문제를 완화시킬 수 있다.

국가 망 보안체계(N²SF)가 제공하는 통제항목을 통해 국가·공공기관은 업무 운영 환경을 효과적으로 구현할 수 있도록 해야 한다. 국가 망 보안체계(N²SF)의 성공적인 구현은 조직의 보안 전략과 기술적 역량의 조화에 있다. 조직은 해당하는 통제 항목을 적용하면 더욱 강력하고 유연한 보안체계를 마련할 수 있을 것이다.

■ 시사점

국가 망 보안체계(N²SF)는 기존의 획일적인 망분리 정책이 가진 한계를 극복하고, 보안성과 데이터 활용성을 동시에 고려한 새로운 보안 패러다임이다. 디지털 전환의 가속화와 함께 AI, 클라우드 등 첨단 기술이 빠르게 확산되는 현시점에서, 공공기관과 국가 차원의 정보보호는 단순한 방어 중심 접근만으로는 한계에 직면하고 있다. 안전한 데이터 활용과 효율적인 업무 환경을 동시에 충족해야 하는 시대적 요구에 따라, 국가 망 보안체계(N²SF)는 망의 등급별 분류와 차등화된 보안 통제를 기반으로 한 혁신적인 방식을 제시하고 있다.

국가 망 보안체계(N²SF)의 도입은 다음과 같은 시사점을 지닌다.

첫째, 보안과 업무 효율성 간의 균형이 가능하다. 망을 기밀(Classified), 민감(Sensitive), 공개(Open) 등급으로 세분화하고, 각 등급에 적합한 보안 대책을 적용함으로써 불필요한 업무 지연이나 비효율을 최소화하는 동시에, 국가 핵심 정보의 안정성을 확보할 수 있다.

둘째, 신기술 도입에 대한 유연성이 향상된다. AI, 빅데이터, 클라우드 등 혁신 기술을 보다 적극적으로 활용할 수 있는 기반이 마련되어, 공공서비스의 품질 제고 및 미래 경쟁력 강화에 기여할 수 있다.

셋째, 보안 위협의 고도화·다변화에 대응하는 체계적인 관리가 가능해진다. 각 망의 특성과 위협 수준을 고려해 맞춤형 보안 정책을 수립함으로써, 사이버 공격에 대한 선제적 대응 역량이 강화된다.

향후 국가 망 보안체계(N²SF)는 국가 및 공공기관뿐 아니라 민간 부문으로도 확산되며, 글로벌 사이버 보안 표준으로 자리매김할 가능성이 높다. 이를 위해서는 제도적 지원뿐 아니라 실무자 교육, 기술 표준화, 정책의 지속적 개선이 병행되어야 한다. 국가 망 보안체계(N²SF)는 단순한 보안 정책을 넘어, 디지털 시대 국가 경쟁력을 좌우하는 핵심 인프라로서 그 중요성이 더욱 커질 것으로 기대된다.

■ 참고문헌

[1] NIST SP 800-207, “Zero Trust Architecture”, 2020.08

[2] NIST SP 800-253, “Cyber Security Framework”, 2020.08

[3] MITRE ATT&CK v14, v15, 2023.10

[4] 국가 망 보안체계 보안 가이드라인(Draft), 2025.01

[5] 국가 망 보안체계 보안 가이드라인(Draft) 부록1, 2025.01