Draft

국가 망 보안체계
보안 가이드라인

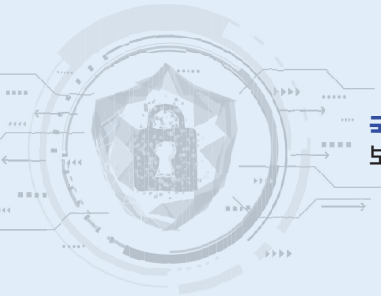
2025. 1

국가정보원 NSR 국가보안기술연구소

Draft

국가 망 보안체계
보안 가이드라인

2025. 1



국가 망 보안체계
보안 가이드라인

문서이력

개정일	버전	내역	비고
2025.1.	Draft	「국가 망 보안체계 보안 가이드라인」 발간	

Summary

1. 목적 및 필요성

본 가이드라인은 공공데이터의 활용을 촉진함과 동시에 보안성을 확보하기 위한 국가 망 보안체계(National Network Security Framework, 이하 N²SF)의 추진배경, 개념, 기본원칙, 적용절차 등을 설명한다.

국가 망 보안체계(N²SF)는 각급기관의 업무를 식별하고 중요도별로 등급을 구분한 후, 해당 등급에 맞추어 보안대책을 차등 적용하는 사이버보안 프레임워크이다.

각급기관은 본 가이드라인에 따라 자율적으로 위협을 식별한 후, 그에 대한 보안대책을 수립하여 보안통제를 선정하고 구현·운영할 수 있다. 이를 위해 국가 망 보안체계에 적합한 보안통제 목록과 C/S/O 보안 등급별 기준선(Baseline)을 제공한다.

또한, 국가·공공기관에서 구축·운영되는 주요 정보서비스 모델에 대해 산·학·연·관 전문가들이 국내·외 위협식별, 위험평가, 관련 규정·지침 분석 등의 과정을 거쳐 수립한 보안통제 항목을 함께 제공한다.

2. 문서의 구조와 기술 범위

1장은 국가 망 보안체계가 등장하게 된 배경을 살펴보고 추진 경과와 추진 목표를 설명한다.

2장은 국가 망 보안체계의 개념, 기본원칙, 보안통제 항목 선택방법 등을 설명한다. 또한, 국가 망 보안체계를 국가·공공기관에 적용하는 절차와 적용·운용 시의 참고사항을 설명한다.

3장은 국가 망 보안체계를 적용하기 위한 각 절차별로 국가·공공기관이 수행해야 할 주요 활동과 그 산출물을 정의한다. 특히, 국가·공공기관이 자율적으로 정보서비스에 대한 위협을 식별하고, 그에 대한 보안대책을 수립하여 보안통제를 선정하는 방법을 제시한다.

이후, 참고에서는 주요국 보안정책 동향 및 접근통제 모델 관점에서의 국가 망 보안체계 등을 설명한다.

CONTENTS

Table List

CONTENTS

Figure List

국가 망 보안체계
보안 가이드라인

제1장

배경

제1절 국가 망 보안정책 개선 추진

제1절

국가 망 보안정책 개선 추진

우리나라는 2006년부터 국가·공공기관 대상 망 분리 정책이 시행되었으며 이후 금융 및 방산 등으로 확대되었다. 각각의 망 분리 정책은 국가정보보안기본지침, 전자금융감독규정, 개인정보보호법 등의 근거에 따른다.

망 분리의 핵심은 민감한 데이터를 다루는 내부망(업무망)을 일반 인터넷망과 분리 운영하여 인터넷을 통한 불법적인 접근이나 정보유출 등 외부로부터의 사이버 위협을 원천적으로 차단하는 것이다.

망 분리 정책은 국내 보안정책의 근간으로 자리 잡아 왔으며 매우 강력한 보안 효과를 보인다는 것이 업계의 중론이다. 실제로, 2017년 전 세계를 강타했던 워너크라이(WannaCry) 랜섬웨어 공격에도 국내의 피해가 미미했던 것은 바로 망 분리 정책의 효과라는 것이 많은 전문가들의 견해이다.

IT 환경의 변화와 현장의 애로사항을 반영해 논리적 망 분리 기술을 추가하고, 망연계 기술 등을 통한 망간 통신을 연계하는 등 망 분리 정책은 시대적 상황에 따라 지속 변화되어왔다.

그러나 최근 원격근무, 클라우드, 생성형 AI 등 IT 환경의 급격한 변화로 인해 인터넷과 단절된 망 분리 환경에서는 업무를 효율적으로 수행하기 어려워지고 있으며, 공공데이터의 대국민 활용 측면에서도 제약이 많아 달라진 업무환경과 신기술을 반영할 수 있도록 망 분리 정책의 개선을 요구하는 목소리가 한층 높아졌다.

이에 따라 국가정보원은 관계기관 및 산학연과 함께 「국가 망 보안정책 개선 합동 TF」를 구성해 민감한 핵심정보는 망 분리가 필요하나, 일반자료는 보안을 완화하여 공공데이터 이용 활성화가 필요하다는 의견을 수렴했다.

그림 1-1 2024년 망 분리 정책 개선 추진 경과

이후 국가정보원은 TF와 합동으로 전산망을 인터넷과 단절된 업무망과 인터넷망으로 분리하는 획일적 망 분리 정책을 개선하기 위해 업무정보의 중요도에 따라 보안통제를 차등 적용하는 '국가 망 보안체계'를 수립하였다.

망 분리 정책 개선은 5가지 목표를 두고 추진하였다.

첫째, 획일적인 망 분리에서 탈피하여 국가 망 보안체계(N^2SF) 기반으로 보안정책의 패러다임을 전환한다.

둘째, 제약 없는 정보유통으로 신기술 융합을 강화하고 스마트 업무환경을 조성한다.

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

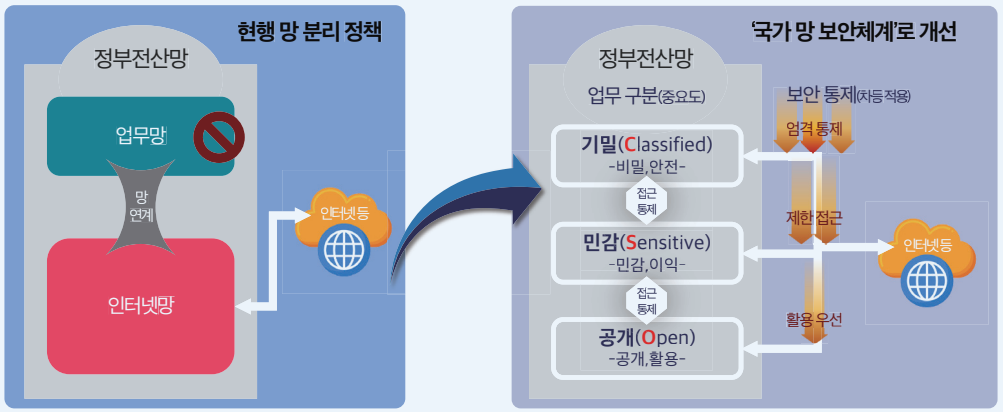
넷째, 새로운 보안정책으로 공표함으로써 각급기관이 제반 여건을 고려하면서 자율적으로 추진하도록 하되, 제도는 점진적으로 변화함으로써 안정적으로 정책이 안착되도록 한다.

다섯째, 공공정보의 보안성과 활용성을 높이는 것과 함께 보안기술 및 AI·데이터 산업 등 다양한 산업발전과 육성으로 디지털경제 창출에도 기여한다.

그림 1-2 망 분리 정책 개선 추진 목표

국가 망 보안체계는 국가·공공기관의 업무정보와 정보시스템에 대해서, 업무 중요도에 따라 기밀(Classified), 민감(Sensitive), 공개(Open) 등 3개 등급으로 분류하고, 등급별로 차등적인 보안통제를 적용하여 보안성 확보와 원활한 데이터 공유의 두 가지 목적을 동시에 달성하는 정책이다.

그림 1-3 기존 망 분리 정책과 국가 망 보안체계 비교



국가 망 보안체계
보안 가이드라인

제2장

국가 망 보안체계(N^2SF) 개요

제1절

국가 망 보안체계 개념

1. 국가 망 보안체계

주요 기반시설과 정부 시스템은 ICT 발전과 고도화라는 시대적 흐름에 따라 사이버공간과 밀접하게 연결되면서 ICT 의존도가 급격하게 높아지게 되었다. 그로 인해 사이버를 포함한 다양한 복합적인 위협에 직면하고 있다.

이러한 위협은 국방, 외교, 행정, 금융 등 국가 핵심 기능을 담당하는 국가·공공기관의 업무와 기능의 연속성을 저해하고 국가안보에 영향을 미칠 수 있는 수준의 위험으로 발전하고 있다.

따라서, 국가·공공기관은 선제적으로 위협을 식별하여, 그로 인한 국가기능의 위험을 파악하고, 신속하게 보호대책을 수립·적용함으로써 조직의 업무와 기능을 보호하고 보안수준을 유지해야 한다.

국가 망 보안체계(N^2SF)는 이를 위한 기본원칙과 세부절차를 제공한다. 국가·공공기관은 국가 망 보안체계를 활용해 위협을 식별하여 보안대책을 수립할 수 있다.

2. 국가 망 보안체계와 정보보안 업무의 관계

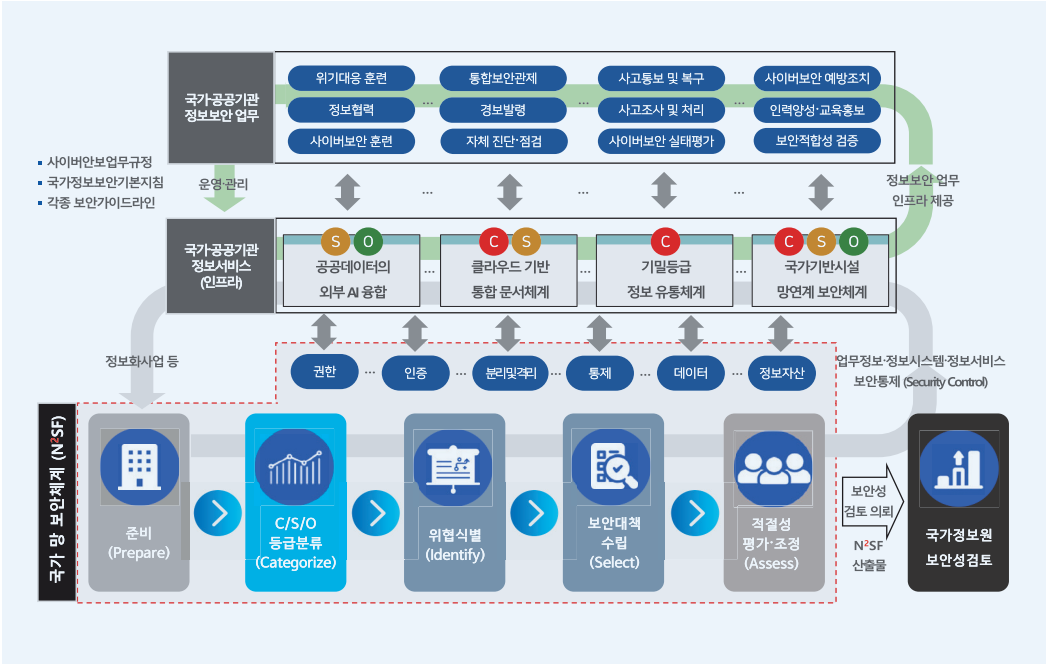
국가·공공기관의 기능 유지를 주목적으로 정보통신망 및 정보시스템을 통해 수집, 가공, 저장, 검색, 송·수신되는 정보의 유출, 위·변조, 훼손 등을 방지하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위와 관련된 업무를 정보보안 업무라 한다.[1]

[그림 2-1]은 국가 망 보안체계와 국가·공공기관의 정보서비스 및 정보보안 업무와의 관계를 나타낸다. 국가·공공기관에서 운영하는 다양한 정보서비스는 정보보안 업무의 인프라에 해당하며,

1 출처: 국가정보보안기본지침 제2조(정의)

국가 망 보안체계는 보안통제를 통해서 정보서비스에 대해 요구되는 보안 수준을 확보하는 역할을 한다.

그림 2-1 국가 망 보안체계와 국가·공공기관 정보보안 업무의 관계



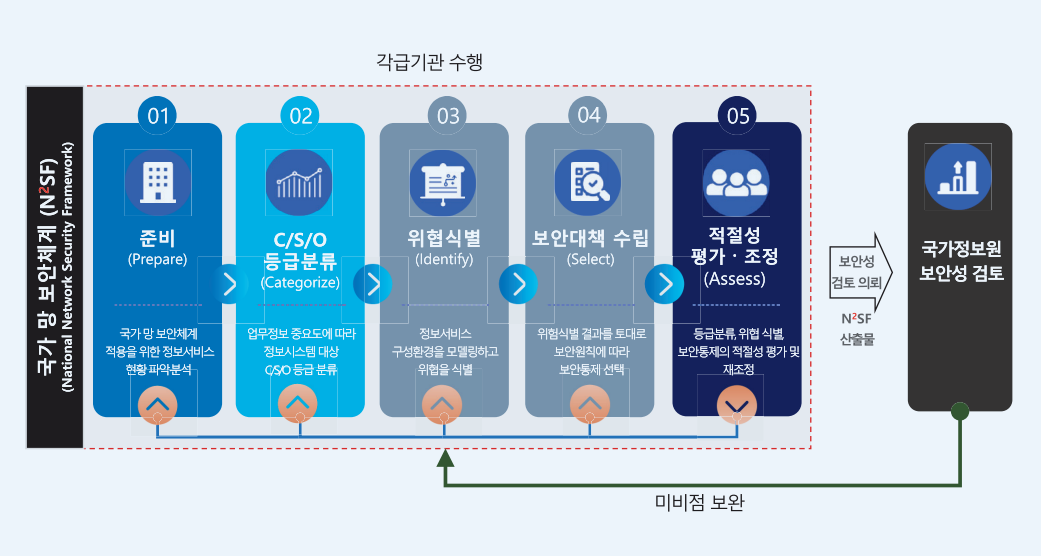
총 5단계의 절차로 적용되는 국가 망 보안체계는 국가·공공기관이 정보화사업을 계획·시행할 때 해당 사업에 포함되는 정보서비스에서 발생할 수 있는 보안 위협을 사전에 식별하여 위험수준을 평가하고 보안대책을 수립하는 과정을 포괄하며, 국가 망 보안체계 각 단계의 산출물은 국가정보보안 기본지침에 따른 국가정보원 보안성 검토 시에 제출하게 된다.

제2절

국가 망 보안체계 적용 절차

국가 망 보안체계는 ①준비, ②C/S/O 등급분류, ③위협식별, ④보안대책 수립, ⑤적절성 평가·조정의 5단계 절차로 수행한다.

그림 2-2 국가 망 보안체계 적용 절차



준비(Prepare) 단계는 기관의 업무정보 및 정보서비스 현황을 식별하고 분석하여 이후 절차에 필요한 기초적인 정보를 확보하고 국가 망 보안체계(N^2SF) 적용 계획을 수립하는 단계이다.

C/S/O 등급분류(Categorize) 단계는 기관의 업무정보 및 정보시스템에 대해 업무 중요도에 따라 C(Classified:기밀), S(Sensitive:민감), O(Open:공개) 등 3개 등급으로 분류한다.

위협식별(Identify) 단계는 정보시스템을 포함한 서비스 환경 전체를 대상으로 모델링 기법을 활용하여 위협을 식별하고, 보안대책 적용이 필요한 대상을 선정한다.

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

마지막으로, 적절성 평가·조정(Assess) 단계에서는 준비, C/S/O 등급분류, 위협식별, 보안대책 수립의 전 과정에 대한 적절성을 평가하고 재조정·승인을 수행한다.

국가 망 보안체계의 모든 단계가 완료되면 절차에 따라 국가정보원 보안성 검토를 요청한다.

이와 같이 국가 망 보안체계는 국가·공공기관이 자산(업무정보·정보시스템·정보서비스)을 분석해 위협을 식별하고 적절한 보안대책을 수립하도록 한다.

제3절

국가 망 보안체계 주요 사항

1. 업무정보와 정보시스템과의 관계

국가의 기능을 수행하는 국가·공공기관의 업무체계는 각급 기관의 조직도, 단위 부서(실·국·과·팀 등)의 수행업무 등과 매우 밀접한 관계가 있으며, 각급 기관의 업무는 업무정보·정보시스템·정보서비스를 통해 동작된다.

따라서, 국가 망 보안체계는 각급 기관의 조직도 및 단위 부서(실·국·과·팀 등)를 기준으로 각급 기관의 업무·기능을 분류하고, 해당 업무·기능을 수행하기 위한 업무정보와, 이에 대한 생성·저장·처리·이동·보관·폐기에 관여하는 정보시스템을 식별할 수 있다. 또한, 이러한 정보시스템들로 구성되는 정보서비스를 식별할 수 있다.

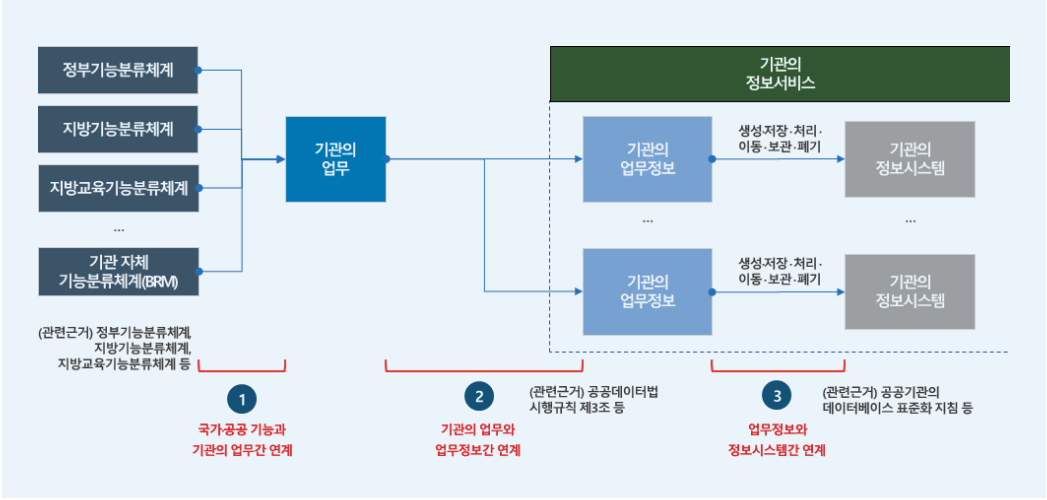
[그림 2-3]은 ❶국가·공공 기능과 기관의 업무, ❷기관의 업무와 업무정보, ❸업무정보와 정보시스템에 이르는 연계성을 설명하고 있다.

첫째, ❶국가·공공 기능과 기관의 업무간 연계는 정부기능분류체계, 지방기능분류체계, 지방교육기능분류체계 등을 기준으로 성립된다.

둘째, ❷기관의 업무와 업무정보간 연계는 공공데이터법 시행규칙 제3조(공공데이터 목록의 등록 서식) 등의 근거로 성립된다. 해당 서식에 따라 각급기관이 보유한 공공데이터(업무정보)의 명칭, 정부기능 분류체계(BRM), 보유근거, 제공대상(미제공시 사유 및 근거 포함) 등을 명세할 수 있다.

셋째, ❸업무정보와 정보시스템간 연계는 공공기관의 데이터베이스 표준화 지침 등의 근거로 성립하며 데이터베이스의 기능, 운영체제, 정부기능 분류체계(BRM) 등 정보시스템에 관한 사항을 기재토록 하고 있다.

그림 2-3 국가·공공의 기능 – 기관의 업무 - 기관의 업무정보·정보시스템·정보서비스 간의관계



2. C/S/O 등급분류 대상

C/S/O 등급분류는 업무정보 및 정보시스템을 대상으로 실시한다. 업무정보의 활용(수집·저장·처리·생성·공유·폐기 등)은 정보시스템의 기능을 통해서 이뤄지고, 이러한 정보시스템의 역기능을 통해 보안문제가 발생할 수 있으며, 정보시스템 또한 업무정보의 C/S/O 등급에 따른 보안대책이 필요하다.

3. 업무정보 C/S/O 등급분류 기준

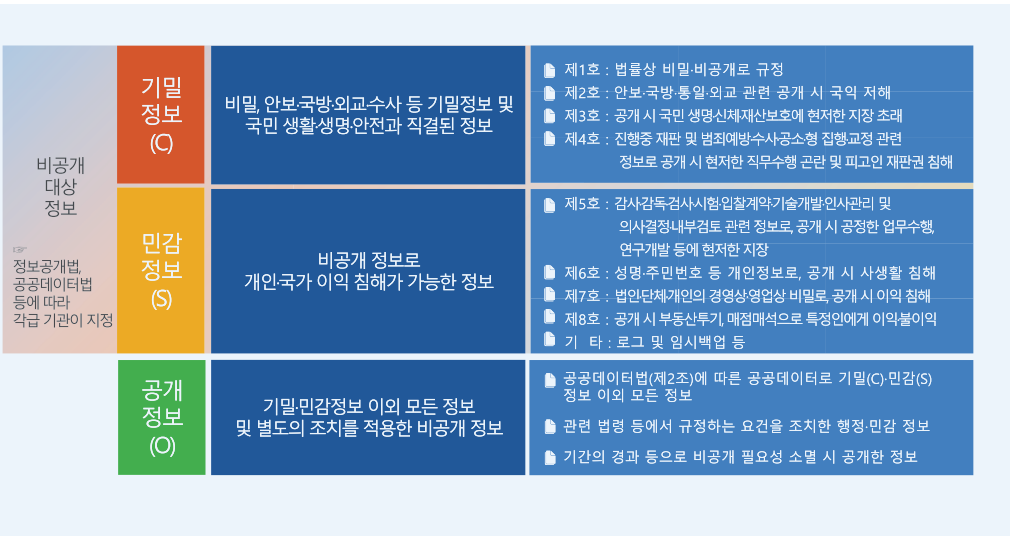
업무정보의 등급 분류는 관련 법령의 근거에 따라 이뤄진다. 기밀정보(C등급)와 민감정보(S등급)는 정보공개법, 공공데이터법, 보안업무규정 등을 근거로 각급기관이 지정한 비공개 정보에 해당한다.

기밀정보(C)는 비밀, 안보·국방·외교·수사 등의 기밀정보와 국민 생활·생명·안전과 직결된 정보로서 정보공개법 제9조(비공개 대상 정보)의 제1호부터 제4호까지를 포함한다.

민감정보(S)는 비공개 정보 등 개인·국가 이익 침해가 가능한 정보로서 정보공개법 제9조(비공개 대상 정보)의 제5호부터 제8호까지의 정보 및 로그, 임시백업 등의 기타 정보를 포함한다.

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

그림 2-4 업무정보에 대한 C/S/O 분류 기준(요약)



* 공공데이터법 및 정보공개법 참조

4. 정보시스템 C/S/O 등급분류 기준

정보시스템의 C/S/O 등급은 기본적으로 [그림 2-5]의 좌측(동일 등급의 경우)과 같이 해당 정보시스템이 포함하는 업무정보의 C/S/O 등급과 동일하게 분류한다.

그림 2-5 정보시스템의 C/S/O 등급분류 기준

그러나, [그림 2-5]의 우측(복수 등급의 경우)과 같이 서로 다른 등급의 업무정보가 포함된 정보시스템의 경우 가장 높은 등급을 해당 정보시스템의 등급으로 분류한다. (Case 1)

단, 이 경우 낮은 등급의 업무정보임에도 높은 등급 수준의 보안대책이 적용될 수 있으므로 동일 등급별로 정보시스템을 분리·운영할 것을 권고한다. (Case 2)

5. 정보서비스 모델링 및 보안원칙 적용을 통한 위협식별

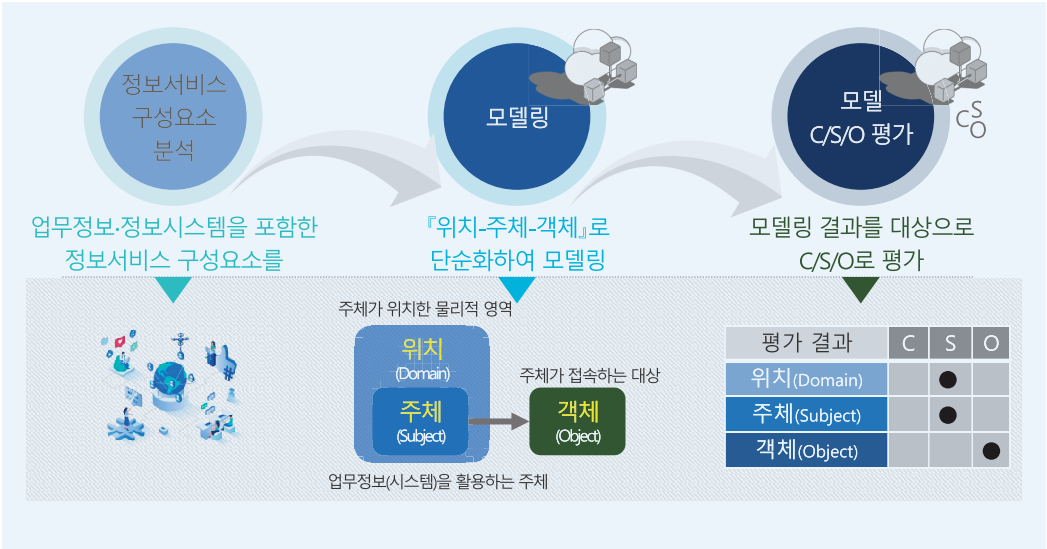
국가 망 보안체계에서는 정보시스템에서 발생 가능한 구조적 위협을 사전에 식별하고 그에 대한 보안대책을 수립하기 위해 위협 모델링을 수행한다. 모델링을 통해 복잡한 실제 정보시스템 구조에서 핵심적인 특징만을 단순하게 표현하여 발생 가능한 보안위협의 존재여부를 판단할 수 있다.

먼저, 정보서비스 구성환경을 「위치-주체-객체」로 단순화하여 표현한다. 여기에서 주체(Subject)는 업무정보·정보시스템을 활용하는 주체(이용자)를 의미하고, 객체(Object)는 주체가 접속하는 대상을

뜻한다. 위치(Domain)는 주체가 위치한 물리적 영역을 나타낸다. 또한 위치, 주체, 객체는 각각 C/S/O 보안등급을 가진다.

따라서, 「위치-주체-객체」로 단순화된 정보서비스 구성환경에 C/S/O등급을 기재하면 해당 정보서비스 환경이 동일한 보안등급으로 구성되는지 또는 서로 다른 보안등급의 위치·주체·객체가 혼용되는지 판단할 수 있다.

그림 2-6 정보서비스 모델링 예시

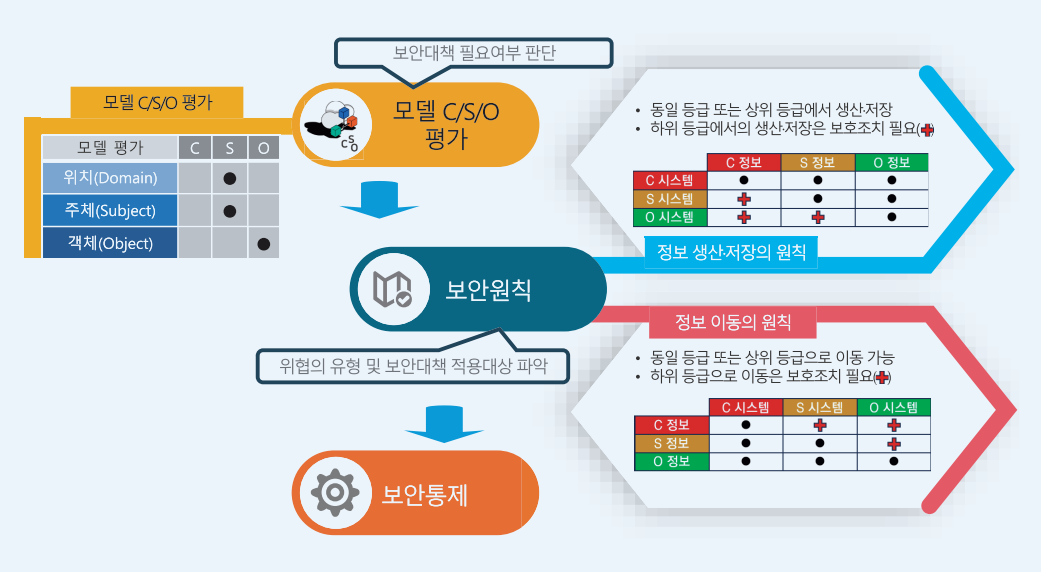


모델링 결과 보안등급의 혼용이 발생하는 경우 보안위협이 존재하며 적절한 보안대책이 요구된다. [그림 2-6]에서 위치와 주체는 모두 S등급이나 객체가 O등급이므로 본 정보서비스 모델은 보안대책을 적용할 필요가 있다.

정보서비스에 대한 「위치-주체-객체」 모델링 및 모델 C/S/O 평가를 수행한 후 서로 다른 보안등급간 혼용이 발생하는 경우, 구체적으로 어떤 업무정보와 정보시스템에 보안위협이 존재하는지, 보안대책 적용이 필요한지 등을 세밀하게 파악할 필요가 있다. 이를 위해, 국가 망 보안체계는 다음 두 가지 보안원칙을 제시한다.

첫째, '정보 생산·저장의 원칙'이다. 기본적으로 정보시스템은 자신의 보안등급과 동일하거나 낮은 보안등급의 업무정보를 생산·저장할 수 있다. 그렇지 않은 경우, 보안대책이 필요하다. ([그림 2-7] 상단의 '✚' 표시)

그림 2-7 정보서비스 모델 대상 보안원칙 적용



둘째, '정보 이동의 원칙'이다. 기본적으로 업무정보는 자신의 보안등급과 동일하거나 높은 보안등급의 정보시스템으로 이동할 수 있다. 그렇지 않은 경우, 보안대책이 필요하다. ([그림 2-7] 하단의 '✚' 표시)

두 가지 보안원칙을 적용하면 위협의 유형과 보안대책 적용대상을 파악할 수 있고, 적절한 보안통제 항목을 선정할 수 있다.

6. 보안통제

보안통제는 정보서비스에서 식별된 위협에 대한 보안대책을 뜻하며, 국가 망 보안체계의 보안통제는 기술적 보안통제를 중심으로 구성된다.

보안통제를 구성하는 각 보안통제 항목은 국가·공공기관의 주요 정보서비스 모델에서 발생할 수 있는 위협의 수준을 완화(예방, 차단, 탐지, 대응, 복구 등)할 수 있도록 설계되었다.

제4절

고려사항

1. 조직의 업무절차와 인식의 틀로 정착 필요

국가 망 보안체계는 국가·공공기관이 일관된 방법으로 정보서비스에 대한 위협을 식별하고 그 위험 수준을 평가하여 적절한 보호대책을 수립·구현·운영하고, 보안수준을 유지할 수 있도록 하는 일련의 지침과 원칙이다.

따라서, 국가 망 보안체계를 통해 국가·공공기관의 보안수준을 실질적으로 향상시키기 위해서는 국가 망 보안체계의 각 단계에서 수행하는 활동을 기관의 실제 정보보안 업무절차에 반영하여 보안에 관한 기본적인 인식의 틀로서 정착될 수 있도록 노력해야 한다.

2. 기관의 특수성 및 상황 반영

보안대책 수립에 있어서 기관별 특성과 사이버공격의 양상 등을 반영할 수 있으며, 보안통제 항목의 선택 및 구현시 조직의 기술적 상황(목표 보안수준, 호환성 등)뿐만 아니라 비기술적 상황(관련규정, 예산, 인력 등)도 함께 고려해 추진하는 것이 바람직하다.

3. 정보서비스 모델

국가·공공기관의 주요 정보서비스 모델에 대한 위협식별 결과, 보안통제 및 구성방안 등 세부사항을 수록한 '정보서비스 모델 해설서'를 제공하므로, 각급기관은 이를 참조하여 해당 정보서비스 환경을 쉽게 구축할 수 있다. 정보서비스 모델은 지속적으로 개발·제공될 예정이다.

국가 망 보안체계
보안 가이드라인

제3장

국가 망 보안체계(N^2SF) 세부 내용

제1절 준비 (Prepare)

제2절 C/S/O 등급분류 (Categorize)

제3절 위협식별 (Identify)

제4절 보안대책 수립 (Select)

제5절 적절성 평가·조정 (Assess)

국가 망 보안체계는 준비(Prepare), C/S/O 등급분류(Categorize), 위협식별(Identify), 보안대책 수립(Select), 적절성 평가·조정(Assess) 등 5단계로 구성된다.

표 3-1 국가 망 보안체계 적용 절차 요약

절차(단계)	주요 활동 (요약)	수행주체
준비 (Prepare)	▸ [NNSF-P-1] N²SF 적용계획 수립 ▸ [NNSF-P-2] 기관 업무·기능 분석 ▸ [NNSF-P-3] 업무정보 식별 ▸ [NNSF-P-4] 정보시스템 식별 ▸ [NNSF-P-5] 정보서비스 식별	각급 기관
C/S/O 등급분류 (Categorize)	▸ [NNSF-C-1] 업무정보 C/S/O 분류 ▸ [NNSF-C-2] 정보시스템 C/S/O 분류	각급 기관
위협식별 (Identify)	▸ [NNSF-I-1] 정보서비스 구성요소 분석 ▸ [NNSF-I-2] 모델링 및 C/S/O 평가 ▸ [NNSF-I-3] 보안원칙 적용	각급 기관
보안대책 수립 (Select)	▸ [NNSF-S-1] 보안통제 선택 ▸ [NNSF-S-2] 보안통제 조정 (필요시) ▸ [NNSF-S-3] 보안통제 구현계획 수립	각급 기관
적절성 평가·조정 (Assess)	▸ [NNSF-A-1] 단계별 적절성 평가 ▸ [NNSF-A-2] 적절성 평가결과 협의·조정(미비점 보완 등) ▸ [NNSF-A-3] 적절성 평가결과 승인	각급 기관

* NNSF: National Network Security Framework

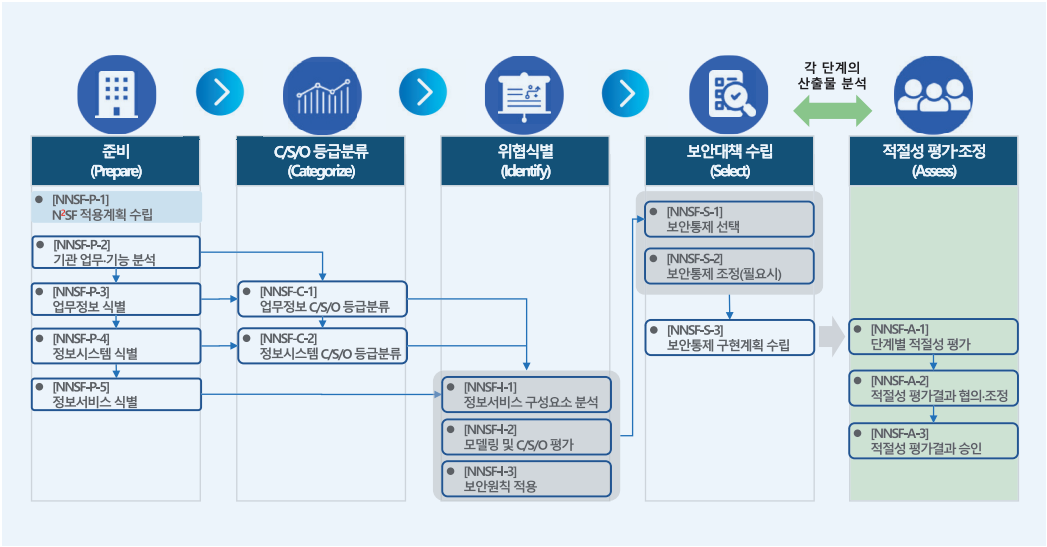
〈표 3-1〉은 각 단계에서 수행하는 주요 활동을 나타낸 것이다. 준비에서부터 적절성 평가·조정에 이르는 전체 절차는 각급기관이 수행한다. 이후 국가정보보안기본지침에 따라 국가정보원 보안성 검토를 거친다.

국가 망 보안체계의 원활한 적용 및 운영을 위해서는 각 단계에서 수행해야 할 주요 활동을 명확히 숙지해야 한다. 또한, 각 활동의 결과를 어떻게 문서화할 것인지 그 형식과 내용을 결정해야 한다.

[그림 3-1]은 단계별 주요 활동간 관계도이다. 각 단계의 활동에서 발생한 산출물은 다음 단계의 활동에 사용되며, 적절성 평가·조정 단계에서 종합적으로 분석된다.

첫째, 준비 단계에서 수행되는 활동의 산출물은 N²SF 적용계획, 기관 기능목록 및 중요도·우선순위, 업무정보(생명주기 포함)·정보시스템·정보서비스 목록이다. 준비 단계의 활동은 국가 망 보안체계 전체 절차를 위한 기초 데이터를 수집하고 N²SF 적용계획을 수립하는 것이다.

그림 3-1 국가 망 보안체계(N²SF) 단계별 주요 활동간 관계도



둘째, C/S/O 등급분류 단계는 준비 단계에서 식별된 업무정보·정보시스템에 관한 C/S/O 등급을 분류한다.

셋째, 위협식별 단계는 업무정보·정보시스템으로 구성되는 정보서비스에 대한 모델링, C/S/O 평가, 보안원칙 적용을 통해 발생 가능한 위협과 보안대책이 필요한 정보서비스 구성요소를 식별한다.

넷째, 보안대책 수립 단계는 위협식별 결과에 따라 업무정보 및 정보시스템에 대한 적절한 보안통제 항목을 선택한다. C/S/O 보안등급별 보안통제 기준선을 활용해서 보안등급에 따른 필요 보안통제 항목을 선택할 수 있고, 기관의 특성 및 정보시스템 환경을 반영한 N²SF 적용계획 등에 따라 보안통제의 제외·수정·추가 등 조정이 가능하다.

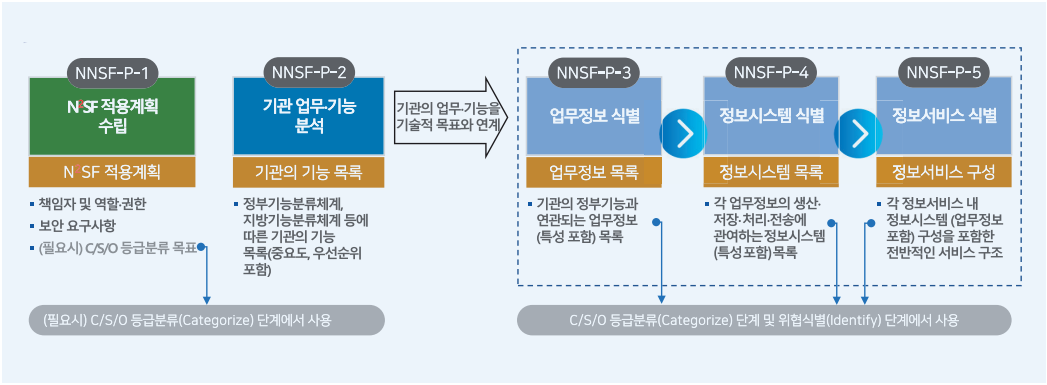
마지막 다섯째, 적절성 평가·조정 단계에서는 앞선 네 단계의 산출물들을 분석하여 단계별 활동이 적절하게 수행되었는지 확인하고 평가한다. 만약, 미흡한 부분이 발견되면 보완할 수 있다. 최종적으로 적절성 평가 결과를 승인함으로써 국가 망 보안체계 적용의 모든 절차를 마친다. 이후 국가정보보안기본지침에 따른 국가정보원 보안성 검토를 시행하게 된다.

제1절

준비 (Prepare)

준비(Prepare) 단계는 국가 망 보안체계 운용에 필요한 기초적인 정보를 수립하고 제반 활동을 준비하는 단계로서 N²SF 적용계획 수립, 기관 업무·기능 분석, 업무정보 식별, 정보시스템 식별, 정보서비스 식별 등 5개 주요활동으로 구성된다.

그림 3-2 준비(Prepare) 단계 주요활동 연계도



준비 단계의 핵심은 정부기능분류체계, 지방기능분류체계, 기관 자체 BRM 등에 따라 기관의 업무·기능을 분석하고 각 기능에 따른 업무정보를 식별하며, 업무정보를 생산·저장·처리·전송하는 정보시스템을 식별한 후, 여러 정보시스템으로 구성된 정보서비스를 파악하여 이후 국가 망 보안체계 수행 절차에 필요한 기반 논리를 구축하는 것이다.

또한, 이를 통해 기관에 적용되는 보안규정, 보안지침 등의 관리적·운영적 목표를 업무정보, 정보시스템, 정보서비스와 같은 기술적 수준의 목표로 연계하고, 필요시 기관의특성을 반영하여 N²SF 적용계획을 수립하는 것은 준비 단계에서 수행하는 매우 중요한 활동이다.

표 3-2 준비(Prepare) 단계의 주요활동 및 산출물

절차(단계)	주요활동	산출물	비고
준비 (Prepare)	[NNSF-P-1] N²SF 적용계획 수립	역할·책임 정의, 자체 심의위원회 구성, 보안요구사항, C/S/O 등급분류 목표(필요시) 등	규정, 지침 등 참고
	[NNSF-P-2] 기관 업무·기능 분석	정부기능 중 기관에 부여된 기능 목록 및 중요도·우선순위	정부기능분류체계 중기능(레벨4) 또는 소기능(레벨5) 수준 이하로 분류된 업무
	[NNSF-P-3] 업무정보 식별	기관의 기능과 연관되는 업무정보(특성 포함) 목록, 공공데이터 목록 등록서(공공데이터법 시행규칙 제3조) 등	
	[NNSF-P-4] 정보시스템 식별	각 업무정보에 대한 생산·저장·처리·전송에 관여하는 정보시스템 목록 및 특성	
	[NNSF-P-5] 정보서비스 식별	각 정보서비스 내 정보시스템(업무정보 포함) 구성을 포함한 전반적인 서비스 구조	

1. N²SF 적용계획 수립 [NNSF-P-1]

N²SF 각 단계의 활동별 책임자를 임명하고 관련된 역할과 권한을 정의한다. 이는 국가 망 보안체계의 특성상 각급기관이 보안대책의 수립, 운영 등에서 자율성과 책임성을 동시에 갖기 위한 것이다.

표 3-3 N²SF 적용계획 수립의 세부 활동

구분	세부 활동	설명	비고
필수	역할 및 책임 정의	N²SF 각 단계의 세부 활동별 책임자 및 역할, 권한 등 정의	객관성 및 책임성 확보를 위해 적절성 평가·조정 단계의 책임자는 기관의 장(또는 CISO, 정보보안담당관)으로 정보보안 업무의 책임자를 지정
		자체 심의위원회 구성 (적절성 평가에 대한 승인 목적)	
필수	보안 요구사항 정의	기관 또는 특정 정보시스템에 요구되는 정보보안·개인정보보호 등 관련 요건 확인	관련 법령, 지침, 가이드라인 등 참고
필요시	C/S/O 등급분류 목표 수립	기관의 업무정보에 대한 C/S/O 등급분류 목표 수준을 사전에 수립	보안 요구사항, 예산 및 기술 현황 등을 고려하여 각 C/S/O 등급으로 분류되는 업무정보의 비율, 개수 등에 관한 목표를 수립

적절성 평가의 최종 승인을 담당할 자체 심의위원회를 구성한다. 심의위원회의 위원장은 기관의 장(또는 CISO, 정보보안담당관)으로 하며 정보화 담당자, 정보화사업 담당자, 정보보안 담당자, 자문위원 등을 포함한다.

그리고, 기관에 적용되는 각종 보안규정, 보안지침, 보안가이드라인 등을 참고하여 기관 전체 또는 특정 정보시스템에 필요한 보안수준을 확인한다.

만약, 요구 보안수준이 N^{2}SF 보안통제 기준선과 차이가 발생한다면, 이후 보안대책 수립 단계에서 보안통제 조정할 수 있으며, 필요시 기관의 C/S/O 등급분류 목표 수준을 사전에 수립할 수 있다.

2. 기관 업무·기능 분석 [NNSF-P-2]

기관의 업무정보를 분석하기 위해서는 정부기능분류체계[2], 지방기능분류체계, 지방교육기능분류체계 등의 기능별 분류를 사용한다. 만약, 보안상의 사유 등으로 이러한 분류체계에 기관의 업무·기능이 충분히 반영되지 않은 경우, 기관의 자체적인 기능분류체계(BRM)를 사용할 수 있다.

[그림 3-3]은 정부기능분류체계를 설명한 것이다. 레벨4(중기능)는 각 부처의 '과' 수준의 기능을 의미하며, 기관의 특성에 따라 하나의 '과'에서 서로 다른 보안등급을 갖는 업무를 수행할 수 있으므로, 이 경우 공개 가능한 업무가 비공개 업무로 판단되거나 비공개 업무가 공개 업무로 판단될 우려가 있다.

따라서, 레벨5(소기능) 이하 수준까지 세분화하여 기관의 업무와 기능을 분류할 것을 권고한다.

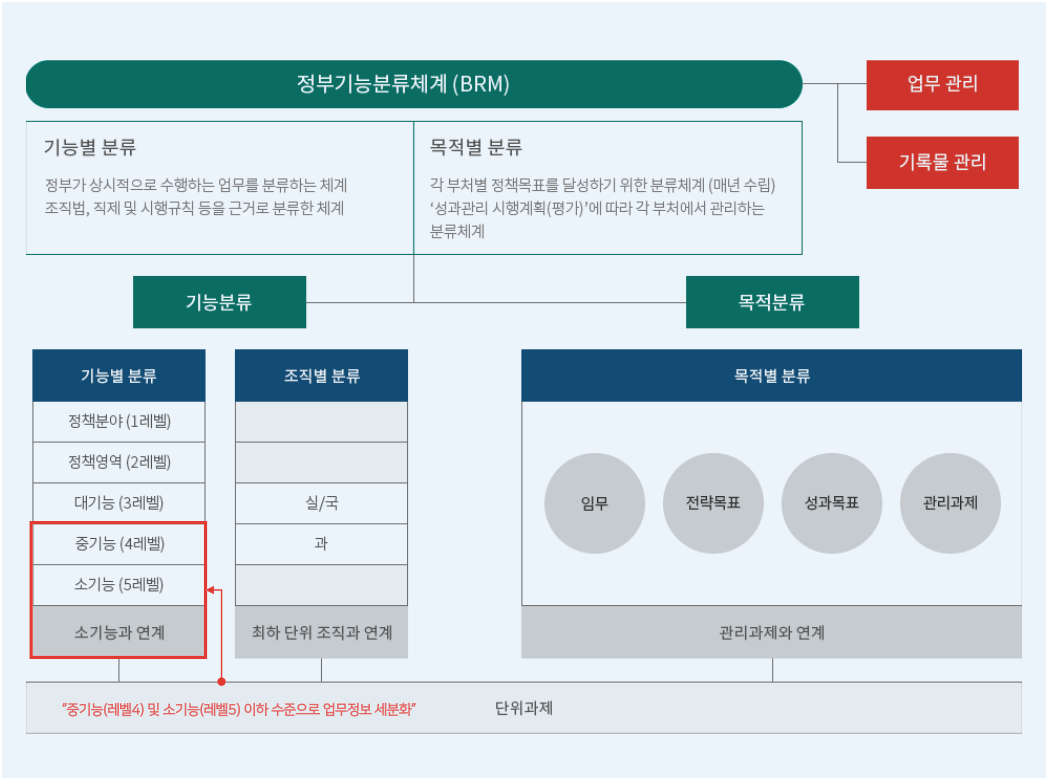
이외 지자체, 교육기관 및 공공기관 등은 정부기능분류체계의 중기능(레벨4) 또는 소기능(레벨5)과 동등하거나 그 이하 수준으로 세분화된 업무정보를 등급분류에 활용하여야 한다. (레벨5 이하 수준 권고)

이와 같이 기관에 따라 정부기능, 지방기능, 지방교육기능 등의 기능분류 체계 또는 자체 BRM 등을 기준으로 업무정보를 목록화하고 각 업무정보에 대한 중요도 및 보호 우선순위를 검토한다. 이렇게 도출된 결론은 이후 업무정보에 대한 C/S/O 등급분류 시에 활용된다.

---

2 관련근거: 정부기능의 분류 및 관리에 관한 규정(행정안전부)

그림 3-3 행정안전부 정부기능분류체계



* 출처: 국가기록원

3. 업무정보 식별 [NNSF-P-3]

업무정보는 국가·공공기관의 기능을 위한 업무를 수행하는데 필요한 정보 또는 그 결과로 생산되는 정보를 의미한다.

[그림 3-4]와 같이 공공데이터 목록 등록 서식(참고: 공공데이터법 시행규칙 제3조)을 이용하여 각급기관의 업무정보를 식별하고, 관련된 정부기능 분류체계 등을 적용하여 C/S/O 등급분류를 위한 기본정보를 구축한다.

그림 3-4 공공데이터 목록의 등록 서식

공공데이터 목록 등록서

「공공데이터의 제공 및 이용 활성화에 관한 법률」 제18조제1항·제27조제5항 및 같은 법 시행령 제15조제1항에 따라 공공데이터 목록을 아래와 같이 등록합니다.

① 공공데이터 목록 명칭(국문)		
② 공공데이터 목록 명칭(영문)		
③ 정부기능 분류체계(BRM)	중기능(레벨4) 및 소기능(레벨5) 이하 권고	
④ 보유 근거(법령)		
⑤ 키워드(3개)		
⑥ 공공데이터 설명		
⑦ 제공대상 여부	제공 [ ]	부분제공 [ ]
	미제공 [ ] 미제공 사유: ( ) 미제공 근거 법률: ( )	
⑧ 향후 제공	향후 제공 [ ] 향후 제공 연도: ( ) 향후 제공 사유: ( )	
⑨ 제공신청에 의한 등록	예 [ ] 아니오 [ ]	

* 참고: 공공데이터법 시행규칙 제3조

또한, 업무정보는 대부분 정보시스템상에서 데이터베이스로 구현되므로, 데이터베이스 수준에서 업무정보를 식별할 수 있어야 한다.

이를 위해, 「공공기관의 데이터베이스 표준화 지침」 등에 따라 국가·공공기관의 데이터베이스는 정부기능분류체계, 지방기능분류체계, 기관자체 BRM 등을 기준으로 기관의 업무를 명시하고 있다.

따라서, 해당 지침을 이용해 기관의 업무를 수행하는데 필요한(또는, 생산되는) 업무정보를 식별할 수 있다.

그림 3-5 공공기관의 데이터베이스 표준화 지침 별표 제4호

구분	항목명	항목 정의 및 작성 지침	
데이터베이스 정의서	기관명	○데이터베이스를 구축한 기관의 이름을 기재	
	부서명	○데이터베이스 구축을 담당한 기관내 조직명을 기재	
	관련법령	○해당 데이터베이스를 구축하고 관리하는 근거 법령을 기재	
	한글 DB명	○기관 자체의 명명규칙을 준수한 논리 데이터베이스 명칭(한글명)을 기재	
	영문 DB명	○정보시스템에서 DB를 식별하기 위하여 사용하는 물리 정보명(영문명)을 기재	
	구축일자	○데이터베이스 구축 일자를 기재 (고도화 사업을 통해 재구축·변경하여 운영 중인 DB의 경우 시스템 고도화 구축 일자)	데이터베이스 수준의 업무정보를 기관의 업무와 연계
	DB 설명	○데이터베이스에서 관리하는 주요 정보의 내용 및 활용·연계 제공 등 데이터베이스의 주요 기능 중심으로 기재	
	업무분류체계	○정부기능분류체계(BRM) 또는 공공기관별 자체 BRM을 참조하여 하위 분류레벨(4단계)까지 기재	
	DBMS 정보	○DBMS(데이터베이스 관리시스템)의 이름 및 버전 등을 기재 -(예시) Oracle 8, DB2 7, Sybase 5, SQL SERVER 8, Informix 7, UniSQL 2, MySQL 5 등	기관특성에 따라, 레벨4 및 레벨5 이하 권고
	운영체제정보	○해당 DBMS가 운영되는 운영 체제의 이름 및 버전을 기재 -(예시) UNIX 5, LINUX 3.1, WINDOWS 2 등	
	DB 형태	○데이터베이스에 저장되는 데이터 형태가 정형인지 비정형인지 구분하여 기재(비정형데이터의 세부유형(공간정보, 문서, 센서(IoT)데이터, 영상, 음성, 이미지, 텍스트)을 추가 기재)	
업무정보가 운용되는 정보시스템에 관한 정보			

* (공공데이터베이스 산출물 표준 관리항목) 발췌

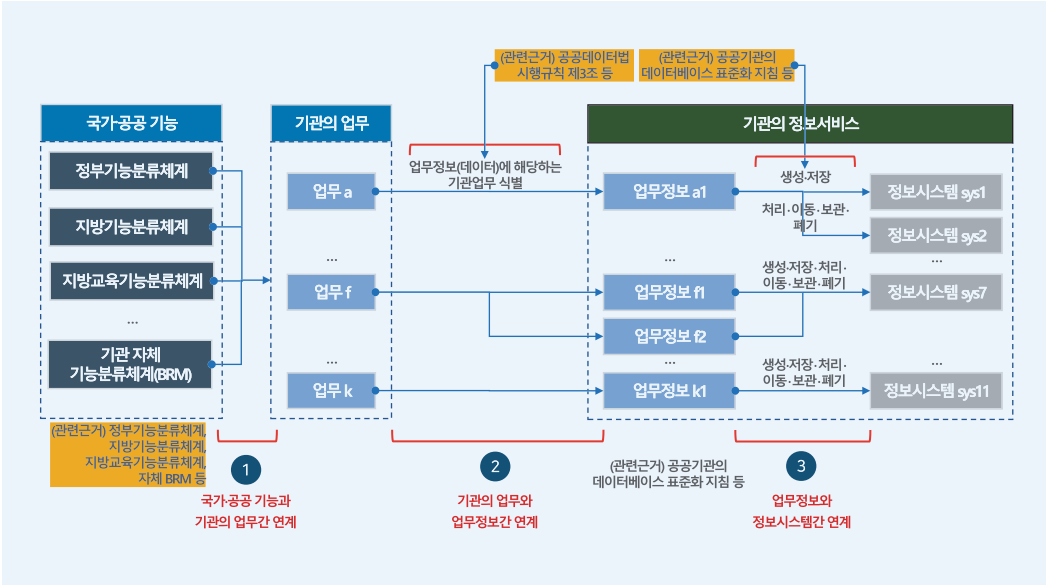
그러나, 「공공기관의 데이터베이스 표준화 지침」에서 데이터베이스 정의서의 업무분류체계는 레벨4(중기능)까지 기재토록 하고 있으나, 국가 망 보안체계에서 각 업무정보는 C/S/O 보안등급을 세밀하게 판단할 필요가 있으므로 레벨5(소기능) 이하 수준까지 식별할 것을 권고한다.

4. 정보시스템 식별 [NNSF-P-4]

정보시스템은 업무정보의 생성·저장·처리·이동·보관·폐기 등에 관여하는 시스템을 뜻하며, 이러한 업무정보의 생명주기를 파악하는 과정에서 업무정보와 관련된 정보시스템을 식별할 수 있게 되며, 각 생명주기에 관련된 정보시스템별로 보안요구사항을 도출할 수 있다.

또한, 업무정보 식별에 근거가 되는 「공공기관의 데이터베이스 표준화 지침」등을 활용하면 해당 업무정보와 관련된 정보시스템의 세부사항(운영체제, DBMS, DB설명, 기관명, 부서명 등)을 식별하고 문서화할 수 있다.

그림 3-6 업무정보를 기준으로 하는 정보시스템 및 정보서비스 식별 개념



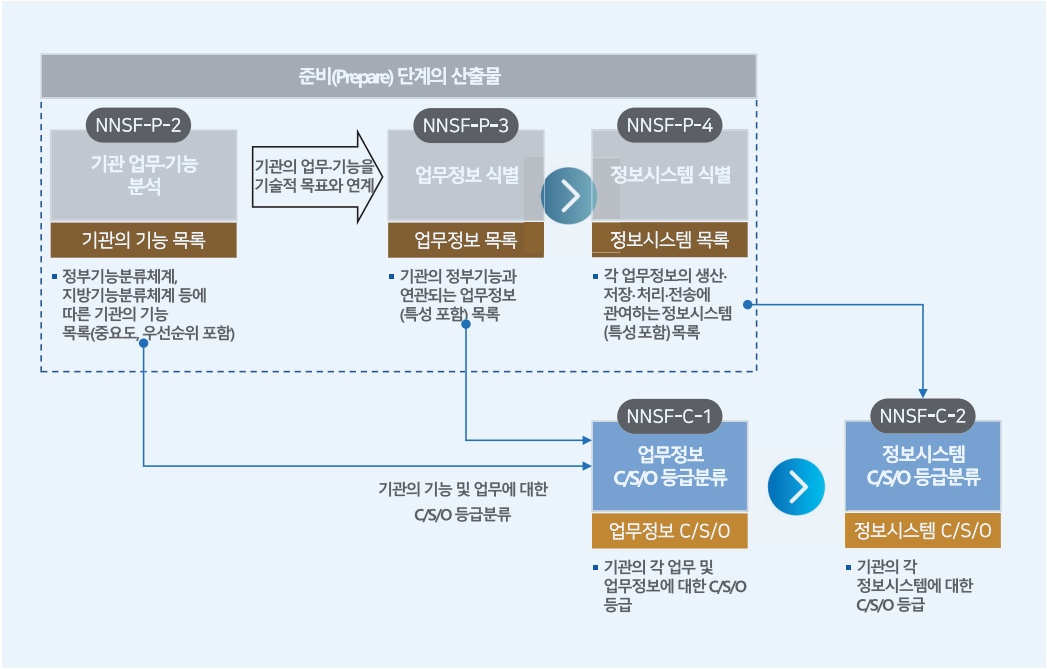
[그림 3-6]은 기관의 업무정보와 정보시스템 간의 관계를 설명하고 있다. '업무 a'는 '업무정보 a1'으로 구성되고 '업무정보 a1'이 '정보시스템 sys1'에서 생성·저장되고, 이후 '정보시스템 sys2'에서 처리·이동·보관·폐기된다면 '정보시스템 sys1'과 '정보시스템 sys2'는 업무정보의 활용 용도가 상이하므로 서로 다른 보안요구사항을 가질 수 있다.

제2절

C/S/O 등급분류 (Categorize)

C/S/O 등급분류(Categorize) 단계에서는 앞선 준비 단계에서 식별한 업무정보 및 업무정보 저장 정보시스템에 대해서 보안등급을 C(기밀), S(민감), O(공개)의 3개 등급으로 분류한다.

그림 3-7 C/S/O 등급분류 단계의 주요활동 및 산출물



준비 단계에서 기관의 기능, 업무, 업무정보, 정보시스템 간의 연계성을 파악하였다. 이를 토대로 업무정보 및 정보시스템에 대한 C/S/O 등급분류를 수행한다.

표 3-4 C/S/O 등급분류(Categorize) 단계의 주요 활동 및 산출물

절차(단계)	주요 활동	산출물	비고
C/S/O 등급분류 (Categorize)	[NNSF-C-1] 업무정보 C/S/O 등급분류	기관의 각 업무 및 업무정보에 대한 C/S/O 등급	
	[NNSF-C-2] 정보시스템 C/S/O 등급분류	기관의 각 정보시스템에 대한 C/S/O 등급	

1. 업무정보 C/S/O 등급분류 [NNSF-C-1]

앞서 준비(Prepare) 단계에서 식별된 기관의 업무에 대해서 다음의 C/S/O 등급분류 기준을 적용하여 등급을 분류한다. 기밀(C) 및 민감(S)은 정보공개법, 공공데이터법, 보안업무규정 등에 의해 각급기관이 지정한 비공개 정보이며, 공개(O)는 그 외의 모든 정보 등이다. C/S/O 등급분류 기준을 법령을 기반으로 상세하게 표시하면 〈표 3-5〉와 같다.

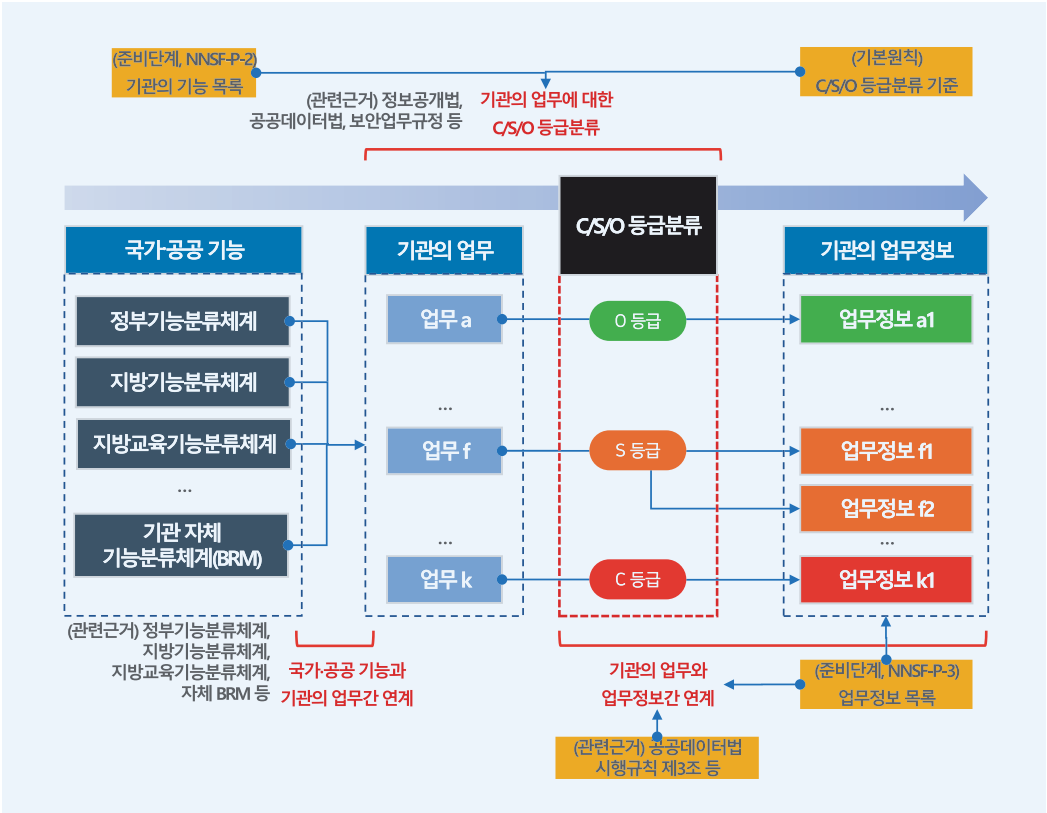
표 3-5 업무정보에 대한 C/S/O 등급분류 기준(상세)

등급	관계 법령에 근거한 C/S/O 등급분류 기준		
기밀 (C)	▸ 제1호: 법률상 비밀·비공개로 규정 ▸ 제2호: 안보·국방·통일·외교 관련 공개시 국익 저해 ▸ 제3호: 공개시 국민 생명·신체·재산보호에 현저한 지장초래 ▸ 제4호: 진행중 재판 및 범죄예방·수사·공소·형집행·교정 관련 정보로, 공개시 현저한 직무수행 곤란 및 피고인 재판권 침해 * (제1항) 다음 중 어느 하나에 해당하는 정보는 비공개 가능	제9조 (비공개 대상 정보)	정보 공개법
민감 (S)	▸ 제5호: 감사·감독·검사·시험·입찰계약·기술개발·인사관리 및 의사결정·내부검토 관련 정보로, 공개시 공정한 업무수행, 연구개발 등에 현저한 지장 ▸ 제6호: 성명·주민번호 등 개인정보로, 공개시 사생활 침해 ▸ 제7호: 법인·단체·개인의 경영상·영업상 비밀로, 공개시 이익 침해 ▸ 제8호: 공개시 부동산투기, 매점매석으로 특정인에게 이익·불이익 * (제1항) 다음 중 어느 하나에 해당하는 정보는 비공개 가능		
	▸ 기 타: 로그 및 임시백업 등 * (제3항) 제1항의 범위에서 공공기관의 업무 성격을 고려해 비공개 대상정보의 범위에 관한 세부기준 수립		
공개 (O)	▸ 비공개 필요성이 소멸된 정보 * (제2항) 기간의 경과 등으로 비공개 필요성 소멸시 공개		
	▸ 기밀(C)·민감(S) 정보 이외의 정보 * (제1항) 공공데이터 이용권의 보편적 확대	제3조 (기본원칙)	공공 데이터법
	▸ 관련 법 등에서 규정하는 요건을 조치한 행정·민감 정보 * 다른 법률에 특별한 규정이 있는 경우를 제외하고 이 법을 따름	제4조 (다른 법률과의 관계)	

[그림 3-8]은 업무정보 C/S/O 등급분류 방법을 나타낸다. 준비단계에서 식별한 기관의 각 업무정보에 대해 C/S/O 등급분류 기준을 적용하여 C/S/O 등급을 분류한다.

기관의 업무에 대한 C/S/O 등급을 결정하면 관련 업무정보의 C/S/O 등급 또한 같은 등급으로 결정된다. 예를 들어, '업무 a'를 O 등급으로 분류했다면 해당 '업무 a'에서 이용(생성, 처리 등)되는 '업무정보 a1'은 '업무 a'와 같은 O 등급으로 결정한다.

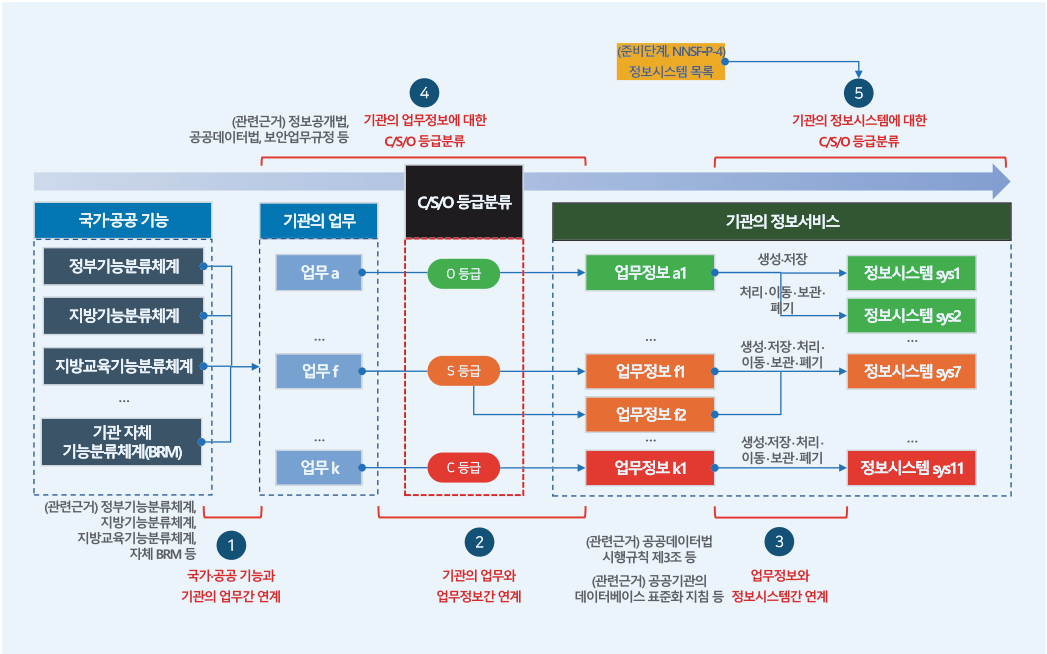
그림 3-8 업무정보 C/S/O 등급분류 방법



2. 정보시스템 C/S/O 등급분류 [NNSF-C-2]

기관 업무정보에 대한 C/S/O 등급분류가 완료된 후 해당 업무정보가 저장된 정보시스템의 등급을 분류한다. 기본적으로는 업무정보의 등급을 정보시스템의 등급으로 반영한다.

그림 3-9 정보시스템 C/S/O 등급분류 흐름 (기관의 업무가 각각 C, S, O로 분류된 경우 예시)



[그림 3-9]는 특정 기관의 '업무 a, f, k'가 각각 O, S, C 등급으로 분류되는 경우 관련된 업무정보와 정보시스템의 등급이 결정되는 모습을 나타낸다. 그림에서 O등급은 녹색, S등급은 주황색, C등급은 적색으로 표시하였다.

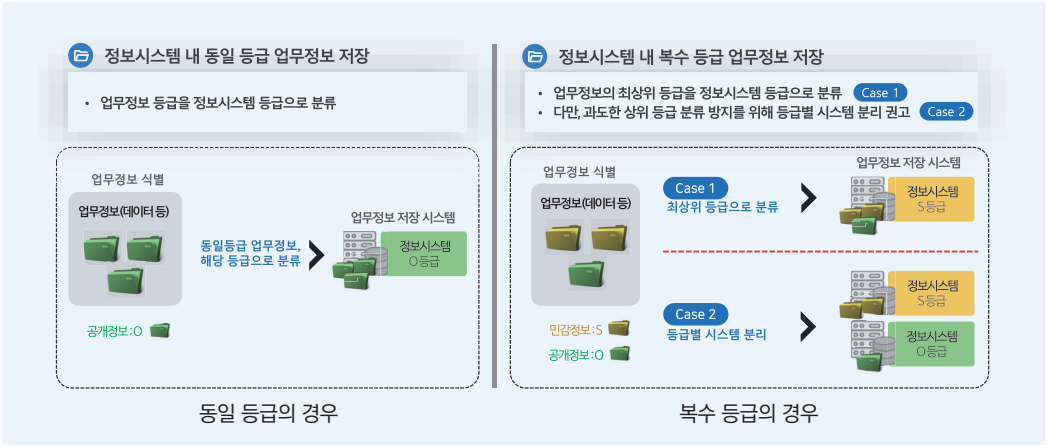
예를 들어, '업무 k'가 C등급으로 분류된다면, '업무 k'에서 이용되는 '업무정보 k1'은 동일하게 C등급으로 분류되고, 해당 '업무정보 k1'의 생성·저장·처리·이동·보관·폐기에 관여하는 '정보시스템 sys11' 또한 C등급으로 분류된다.

그러나, 1개 이상의 업무정보를 포함하여 정보시스템을 구축·운영하는 경우, 각 업무정보의 등급에 따라 정보시스템의 등급분류 방법이 달라진다.

[그림 3-10]은 동일 등급의 업무정보로 구성된 정보시스템과 복수 등급의 업무정보로 구성된 정보시스템에 대한 각각의 C/S/O 등급분류 방법을 설명하고 있다.

하나의 정보시스템에 동일 등급의 업무정보가 저장된 경우, 해당 업무정보 등급을 정보시스템 등급으로 반영한다. 예를 들어, 기상정보를 저장하는 데이터베이스 서버의 경우, 기상정보가 O등급으로 분류되었다면 데이터베이스 서버 또한 O등급으로 분류한다.

그림 3-10 정보시스템의 C/S/O 등급분류 기준



복수 등급의 경우 두 가지 방법(Case 1, Case 2)을 적용할 수 있는데, 이에 대한 장단점 및 주의사항을 정리하면 〈표 3-6〉과 같다.

첫째, Case 1은 가장 높은 등급을 해당 정보시스템의 등급으로 분류하는 것이다. 이 방법은 가장 간단하고 보안성은 높지만, 낮은 등급의 업무정보가 과도하게 높은 등급으로 분류될 수 있다.

둘째, Case 2는 동일 등급의 업무정보별로 정보시스템을 분리하는 것이다. 이 방법은 정보시스템 단위로 보안통제 적용 및 보안관리로 보안 측면에서 가장 명확한 분류 방법이나 정보시스템 구성의 변화에 따른 개발, 유지보수 등의 추가 비용이 소요될 수 있다.

표 3-6 정보시스템에 대한 C/S/O 등급분류 경우의 수 및 주의 사항

구성	업무정보 보안등급	조건	정보시스템 보안등급		비고(주의 사항)
하나의 정보시스템에 동일 등급 업무정보 포함 시	C	-	C		
	S	-	S		
	O	-	O		
하나의 정보시스템에 복수 등급 업무정보 포함 시	S + O	Case 1 상위등급으로 분류	S		과도한 상위등급 분류
		Case 2 시스템 분리	S	O	시스템 분리에 따른 비용 소요
	C + S	Case 1 상위등급으로 분류	C		과도한 상위등급 분류
		Case 2 시스템 분리	C	S	시스템 분리에 따른 비용 소요
	C + O	Case 1 상위등급으로 분류	C		과도한 상위등급 분류
		Case 2 시스템 분리	C	O	시스템 분리에 따른 비용 소요

제3절

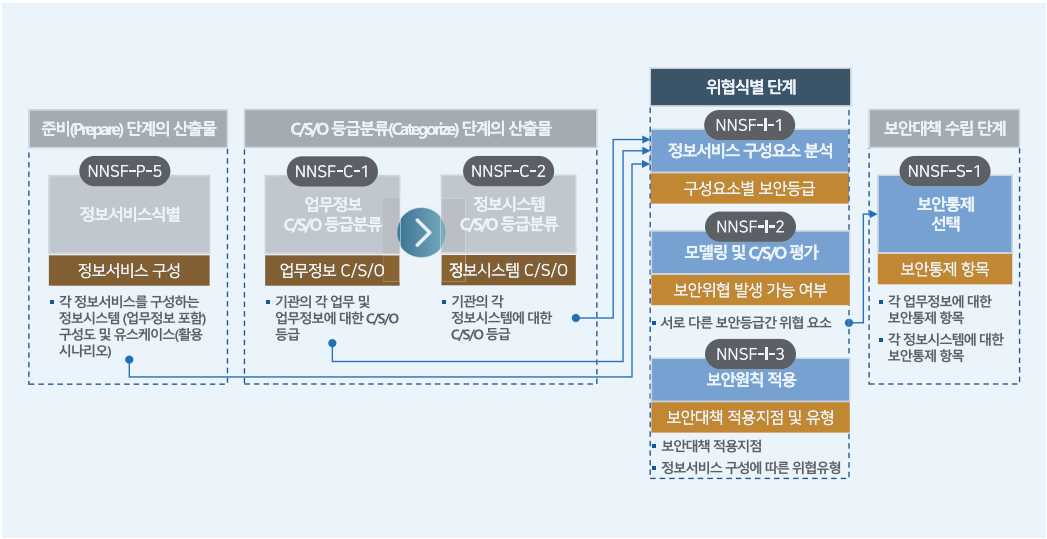
위협식별 (Identify)

위협식별(Identify) 단계에서는 서로 다른 보안등급간 위협요소를 식별하고 보안대책 적용 구성요소(지점)를 발견하기 위한 위협 모델링을 수행한다.

정보서비스 위협 모델링을 위해서는 준비 단계에서 식별한 정보서비스 구성 정보와 C/S/O 등급 분류 단계에서 결정된 업무정보 C/S/O, 정보시스템 C/S/O 등이 필요하다.

정보서비스 위협 모델링을 수행하면 그 결과로 서로 다른 보안등급이 식별되어 보안대책 적용 지점을 도출할 수 있으며, 보안통제 기준선과 이를 통해서 보안통제 항목 선택이 가능해진다.

그림 3-11 위협식별 단계의 주요활동 연계도



위협을 식별하고 그 위험을 평가하며 적절한 보안통제를 선택하는 데 있어서, 모든 국가·공공기관에 적합한 기술적 수준의 방법론을 제시하는 것은 매우 어려운 일이다.

왜냐하면 교육, 전력, 과학, 치안, 복지 등 공공 부문별 산업군과 그에 따른 기관의 업무와 기능이 서로 다르며, 기관별로 다루는 업무정보와 이를 저장·처리하는 정보시스템의 형상, 정보시스템을 구성하는 HW·SW, 정보시스템을 기반으로 동작하는 정보서비스의 기술적·운영적 특성이 서로 다르기 때문이다.

따라서, 국가 망 보안체계는 모든 국가·공공기관에 공통적으로 적용할 수 있는 정보서비스 위협 식별 방법론으로 「위치-주체-객체」 모델링을 제시하며, 세부적인 보안원칙으로서 「정보 생산·저장」 원칙, 「정보 이동」 원칙을 제시한다.

표 3-7 위협식별(Identify) 단계의 주요 활동 및 산출물

절차(단계)	주요 활동	산출물	비고
위협식별 (Identify)	[NNSF-I-1] 정보서비스 구성요소 분석	정보서비스 구성(보안등급 포함) 및 서비스·기능	주요 보안 특성을 형상화하기 위한 모델링
	[NNSF-I-2] 모델링 및 C/S/O 평가	「위치-주체-객체」 모델	
		모델 C/S/O 평가결과 (서로 다른 등급 혼재 여부)	서로 다른 보안등급간 위협 식별
	[NNSF-I-3] 보안원칙 적용	「정보 생산·저장」시 위협 (위협유형 및 위협 발생지점)	정보 생산·저장 시 위협 식별
		「정보 이동」시 위협 (위협유형 및 위협 발생지점)	정보 이동 시 위협 식별

위협식별 단계의 상세한 과정을 설명하기 위해 [그림 3-12]와 같이 기관 전산망에서 인터넷을 통해 생성형 AI 서비스를 활용하는 정보서비스 모델을 예시로 이용한다.

그림 3-12 정보서비스 모델(예시, 이후 지속 참조)

1. 정보서비스 구성요소 분석 [NNSF-I-1]

정보서비스를 구성하는 정보시스템을 식별하고, 정보서비스의 기능 및 유스케이스(정상적인 사용 시나리오)에 따른 구성요소를 분석한다.

표 3-8 정보서비스 모델(예시)의 구성요소

위치	구성요소
인터넷망	생성형AI서비스(시스템)
기관전산망	업무시스템
	업무단말
	온북
	기관전산망-인터넷망 연계구간(NW)
	기관전산망 내부구간(NW)

예로 제시된 정보서비스 모델의 구성요소는 〈표3-8〉과 같으며, 이용자는 기관전산망에서 업무단말 및 온북을 이용해서 생성형 AI 서비스에 접속, 업무정보를 업로드하여 AI 서비스를 통해 새로운 업무정보를 생산한다.

2. 모델링 및 C/S/O 평가 [NNSF-I-2]

「위치-주체-객체」 모델링은 정보서비스의 위치와 이를 이용하는 주체(이용자[3])가 직접 이용하는 단말·서버, 그리고 정보서비스가 접근하는 객체를 식별한다.

주체(Subject)는 업무정보·정보시스템을 활용하는 주체(이용자)를 의미하고, 객체(Object)는 주체가 접속하는 대상을 뜻한다. 위치(Domain)는 주체가 위치한 물리적 영역을 나타낸다.

그 후, 위치·주체·객체의 보안등급(C/S/O)을 각각 식별하고, 「위치-주체-객체」 모델 평가표에 식별된 정보를 기재하여 위치·주체·객체가 모두 동일 등급에 위치하는지 확인한다.

[그림 3-13]은 예시로 제시된 정보서비스 모델에 대한 「위치-주체-객체」 모델링과 C/S/O 평가 과정을 나타낸다.

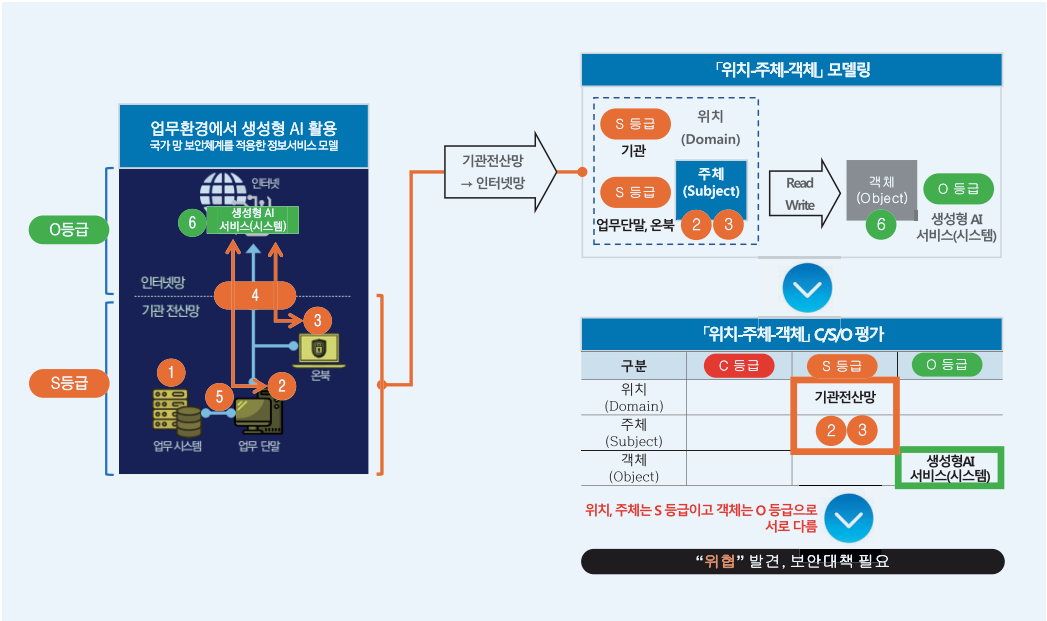
기관전산망(S등급)에서 업무단말(S등급) 및 온북(S등급)을 이용해서 인터넷에 위치한 생성형 AI 서비스(O등급)를 이용하는 유스케이스(활용 예)이므로, 위치(기관전산망)와 주체(업무단말❷ 및 온북❸)는 모두 S등급이고 객체(생성형 AI 서비스❻)는 O등급에 해당한다.

이를 「위치-주체-객체」 모델 C/S/O 평가에 대입하면 S등급과 O등급에 걸친 형태이므로 위협 발생 가능성이 있어 보안대책이 필요하고, 구체적인 위협의 양상과 보안대책 적용지점을 파악하기 위해 다음 단계의 보안원칙 적용을 수행해야 한다.

---

3 이용자는 정상적인 권한을 가지고 정상적인 절차로 정보서비스를 이용하는 것으로 가정한다. 그렇지 않으면 내부자 위협을 모델링 단계에서 다뤄야 하는데 이는 모델링 과정을 매우 복잡하게 할 수 있다. 이를 위해 내부자 위협에 대한 보안대책은 기본적인 보안통제 기준선(Baseline)에 반영한다.

그림 3-13 「위치-주체-객체」 모델링 및 C/S/O 평가를 통한 위협식별



3. 보안원칙 적용 [NNSF-I-3]

가. 「정보 생산·저장」 보안원칙 적용

「정보 생산·저장」 보안원칙은 정보서비스를 구성하는 각 정보시스템에서 업무정보가 생산·저장될 때, 정보시스템의 보안등급보다 높은 등급의 업무정보가 생산·저장되는 것을 위협으로 식별한다. 위협식별 영역에는 '✚' 표시가 있다.

「정보 생산·저장」 보안원칙			
~에서 생산저장	C 정보	S 정보	O 정보
C 시스템	●	●	●
S 시스템	✚	●	●
O 시스템	✚	✚	●

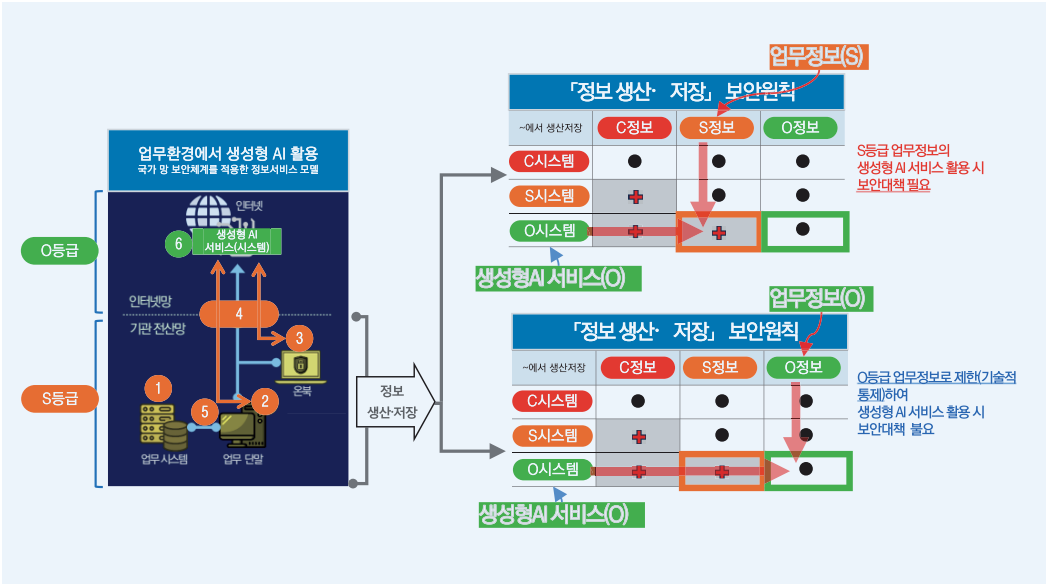
[그림 3-14]는 예시로 제시된 정보서비스 모델에 대한 「정보 생산·저장」 보안원칙 적용 과정을 나타낸다.

S등급 업무정보를 생성형AI 서비스에 활용하는 경우 생성형AI 서비스(O등급)에서 S등급 업무정보가 생산·저장되는 위협을 발견할 수 있으며, 생성형 AI 서비스⑥에서 보안대책이 필요함을 알 수 있다.

그러나, 만약 O등급 업무정보를 생성형AI 서비스에 활용하는 경우라면 O등급 정보시스템에서 O등급 업무정보가 생산·저장되므로 위협이 발견되지 않는다.[4]

따라서, 정밀한 위협식별을 위해서는 정보서비스 유스케이스(사용 시나리오)를 세분화하여 분석할 필요가 있다.

그림 3-14 「정보 생산·저장」 보안원칙을 적용한 위협식별 및 보안대책 적용지점 판단



나. 「정보 이동」 보안원칙 적용

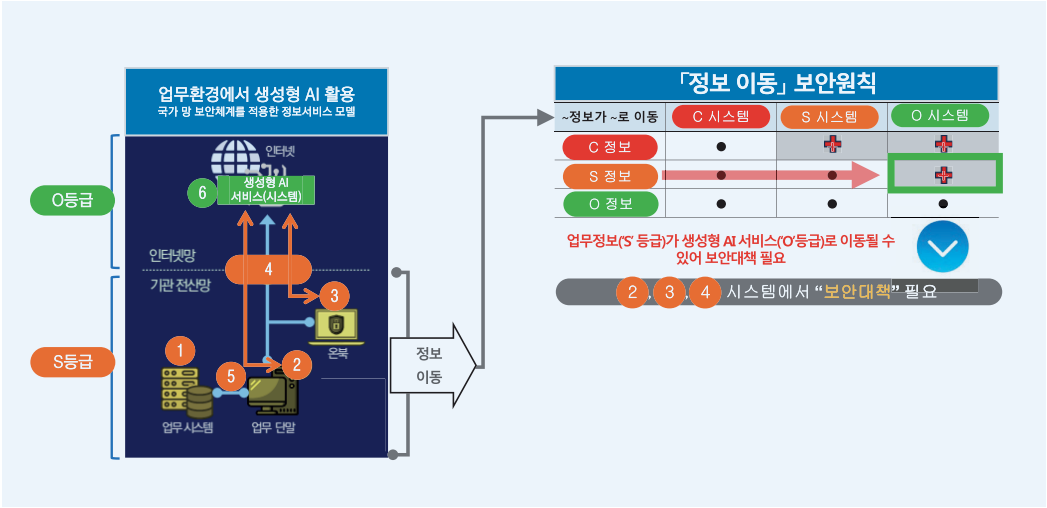
「정보 이동」 보안원칙은 업무정보가 각 정보시스템으로 이동할 때, 업무정보의 보안등급보다 낮은 등급의 정보시스템으로 이동이 발생하는 것을 위협으로 식별한다. 마찬가지로, 위협식별 영역에는 '✚' 표시가 있다.

4 위협식별 단계에서 위협이 발견되지 않은 경우에도 정보서비스의 각 구성요소에 대해 C/S/O 등급별 보안통제 기준선에 따른 보안대책은 우선적으로 적용을 검토해야 한다.

「정보 이동」 보안원칙			
~정보가 ~로 이동	C 시스템	S 시스템	O 시스템
C 정보	●	✚	✚
S 정보	●	●	✚
O 정보	●	●	●

[그림 3-15]는 예시로 제시된 정보서비스 모델에 대한 「정보 이동」 보안원칙 적용 과정을 나타낸다. 업무단말❷과 온북❸에서 생성형 AI 서비스❻로 업무정보(S등급)를 업로드하여 처리·가공할 수 있으므로 위협으로 식별된다.

그림 3-15 「정보 이동」 보안원칙을 적용한 위협식별 및 보안대책 적용지점 판단



구체적으로 업무정보를 업로드하는 업무단말❷과 온북❸, 그리고 업무정보가 통과하는 기관전산망-인터넷망 연계구간(NW)❹에서 보안대책이 필요함을 알 수 있다.

제4절

보안대책 수립 (Select)

보안대책 수립 단계에서는 앞선 정보서비스 모델링 단계에서 식별된 위협요소와 보안대책 적용지점에 관한 정보를 토대로, 각 업무정보·정보시스템에 대한 보안통제 항목을 선택·조정한 후, 보안통제 구현계획을 수립한다.

그림 3-16 보안대책 수립 단계의 주요활동 연계도

표 3-9 보안대책 수립(Select) 단계의 주요 활동 및 산출물

절차(단계)	주요 활동	산출물	비고
보안대책 수립 (Select)	[NNSF-S-1] 보안통제 선택	각 업무정보에 대한 보안통제 항목	보안통제 항목 해설서 참조
		각 정보시스템에 대한 보안통제 항목	보안통제 항목 해설서 참조
	[NNSF-S-2] 보안통제 조정	N^2SF 적용계획 등에 따라 조정된 보안통제 항목	
	[NNSF-S-3] 보안통제 구현계획 수립	보안통제 구현계획	

1. 보안통제 선택 [NNSF-S-1]

앞서 위협식별 단계에서 식별된 보안대책 적용지점에 국가 망 보안체계(N^2SF) 보안통제를 통해서 보호대책을 적용한다. 또한 필요시 N^2SF 보안통제 외에 관련 법령·규정 등에서 요구하는 추가적인 방안이 적용될 수도 있다.

가. 보안통제 기준선(Baseline) 활용

[그림 3-17]은 국가 망 보안체계에서 사용되는 보안통제 항목 구성 예시이다. 각 보안통제 항목은 관리 용이성을 위해 고유한 N^2SF ID를 가진다.

그림 3-17 국가 망 보안체계 보안통제 구조

국내 보안정책 반영
- 국가정보보안기본지침
- 각종 보안가이드라인 등

대항목	중항목	N²SF 보안통제 ID	소항목	N²SF 보안통제 기준선(Baseline)			설명
				O (공개)	S (민감)	C (기밀)	
인증	다중요소 인증	NNSF-MA-1	관리자 계정 다중요소 인증(MFA, Multi-factor Authentication)	●	●	●	
		NNSF-MA-2	사용자 계정 다중요소 인증(MFA, Multi-factor Authentication)	●	●	●	
		NNSF-MA-3	다중요소 인증 장치 분리			●	
		NNSF-MA-4	다중요소 인증(MFA, Multi-factor Authentication) 경로 분리		●	●	
...							
통제	원격접속	NNSF-RA-1	원격접속 모니터링 및 통제		●	●	
		NNSF-RA-2	원격접속 세션 암호화		●	●	

보안통제 분류 / 보안통제 제목 / C/S/O 등급별 기본 보안통제

또한, 보안통제 기준선(Baseline)은 등급별 우선 검토해야 하는 보안통제 항목으로 정보서비스 구성, 운용환경 및 기관 특성 등을 고려하여 보안통제 항목을 조정·반영할 수 있다.

보안통제 기준선(Baseline)에는 C(기밀)·S(민감)·O(공개) 등급별로 우선 적용을 검토하는 보안통제 항목은 '●' 표기하고, 사용 제한을 권고하는 항목은 '-'로 표기하였으며 국내 보안정책(국가정보보안기본지침, 보안가이드라인 등) 및 미국 등 해외 보안정책을 분석, 최적화하였다.

[그림 3-18]는 국가 망 보안체계에서 보안통제 항목을 선택하는 방법을 나타낸 것이다. C/S/O 등급별 기준선에 따라 ● 표시가 되어있는 보안통제 항목을 선택한다.

예를 들어, [그림 3-18]와 같이 S등급으로 분류된 업무정보·정보시스템에 대해서는 S등급 기준선(Baseline) 해당란에 ● 표시가 되어있는 보안통제 항목을 우선적으로 선택한다. 이후 준비단계에서 수립된 N²SF 적용계획, 보안요구사항 등에 따라 보안통제 항목의 적용여부, 적용수준 등을 조정할 수 있다.

그림 3-18 국가 망 보안체계 보안통제 항목 선택 방법

대항목	중항목	N²SF 보안통제 ID	소항목	N²SF 보안통제 기준선(Baseline) O (공개)	S (민감)	C (기밀)	설명
인증	다중요소 인증	NNSF-MA-1	관리자 계정 다중요소 인증(MFA, Multi-factor Authentication)	●	●	●	
		NNSF-MA-2	사용자 계정 다중요소 인증(MFA, Multi-factor Authentication)	●	●	●	
		NNSF-MA-3	다중요소 인증 장치 분리			●	
		NNSF-MA-4	다중요소 인증(MFA, Multi-factor Authentication) 경로 분리		●	●	
...							
통제	원격접속	NNSF-RA-1	원격접속 모니터링 및 통제		●	●	
		NNSF-RA-2	원격접속 세션 암호화		●	●	

* 예: 'S'등급 업무정보·정보시스템

나. 정보서비스 모델 해설서 참조

본 가이드라인에 포함된 정보서비스 모델과 동일 또는 유사한 경우 해설서를 참조하여 보안통제 항목을 선정할 수 있다.

2. 보안통제 조정 [NNSF-S-2]

위협식별 단계에서 식별된 보안대책 적용지점에 기관에 임무, 중요도, 우선 순위 등을 반영하여 국가 망 보안체계(N²SF) 보안통제 항목을 조정할 수 있다.

3. 보안통제 구현계획 수립 [NNSF-S-3]

〈표 3-10〉은 보안통제 구현계획 수립에 포함되는 세부활동을 나열한 것이다.

표 3-10 보안통제 구현계획 수립의 세부 활동

구분	세부 활동	설명	비고
필수	구현 우선순위 설정	기관의 업무·기능 중요도 및 우선순위에 따라 해당 업무정보·정보시스템의 보안통제 우선순위 결정	준비단계의 기관 업무·기능 분석, 업무정보 식별, 정보시스템 식별 등의 산출물 활용
필수	책임자 및 자원 할당	각 보안통제를 담당할 책임자를 지정하고, 통제구현에 필요한 인력, 기술, 예산 등을 배정	
필수	구현방법 정의 및 기술적 요구사항 파악	보안통제를 시스템에 적용하기 위한 구체적인 방법론, 절차, 기술적 요구사항(호환성 등) 정의	보안설정, 보안기능 개발, 상용 보안제품 도입, 매니지드 보안 서비스 등
필수	구현일정 수립	각 보안통제에 대한 구현일정 설정	구현 우선순위와 연계
필요시	위험감소 효과 예상	보안통제 구현을 통해 위험수준을 어떻게 감소시킬 수 있을지 예측	N²SF 절차 이후 보안성검토 완료 후, 보안통제가 구현되고 운용되는 단계에서의 상시적인 평가시 활용

구현 우선순위 설정은 기관의 업무·기능 중요도 및 우선순위에 따라, 해당 업무·기능과 연계된 업무정보·정보시스템에 대한 보안통제의 우선순위를 결정한다. 또한, 기관이 가진 인력·기술·예산 등의 상황도 함께 고려되어야 한다.

제5절

적절성 평가·조정 (Assess)

국가 망 보안체계의 전체 단계에서 요구되는 활동이 올바르게 이뤄졌는지 각 활동 결과(산출물)를 통해 평가하고 미흡한 점에 대해서는 조정해서 보완한다.

그림 3-19 적절성 평가·조정 단계 요약

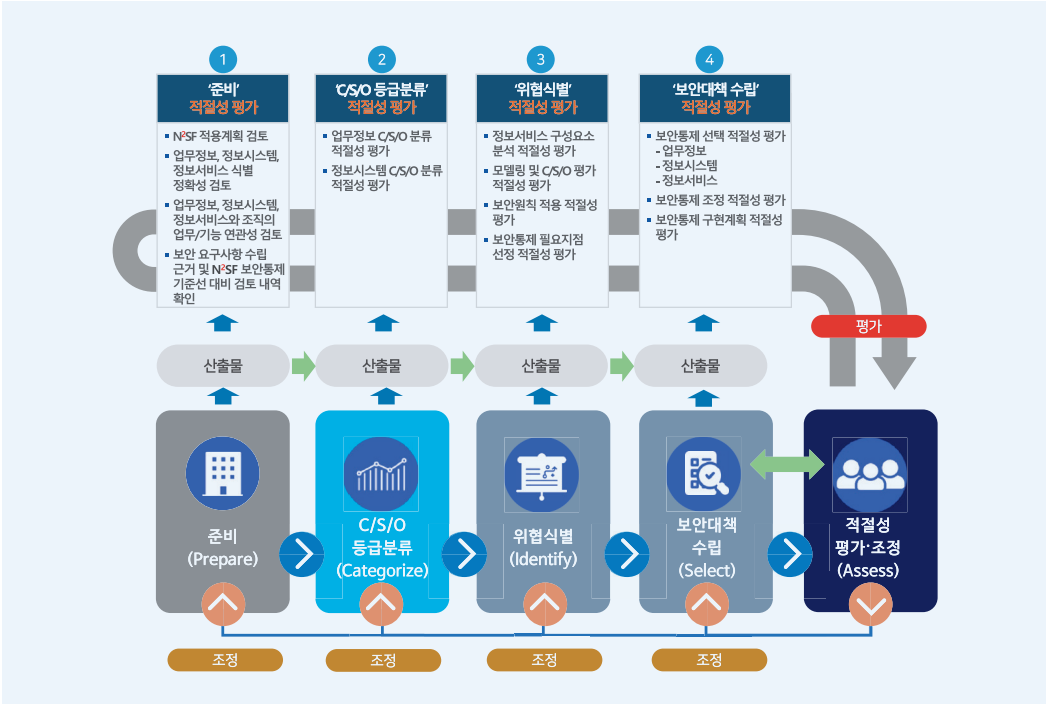


표 3-11 적절성 평가·조정(Assess) 단계의 주요 활동 및 산출물

절차(단계)	주요 활동	산출물	비고
적절성 평가·조정 (Assess)	[NNSF-A-1] 단계별 적절성 평가	적절성 평가 보고서	
	[NNSF-A-2] 적절성 평가결과 협의 및 조정	적절성 평가결과 협의·조정 내역	
	[NNSF-A-3]적절성 평가결과 승인	적절성 평가결과 승인서	자체 심의위원회

1. 단계별 적절성 평가 [NNSF-A-1]

국가 망 보안체계는 각 단계별로 주요활동과 그 결과로 생성되는 산출물이 정의되어 있다. 따라서, 각 활동의 산출물을 확인하면 단계별 활동의 적절성을 평가할 수 있다.

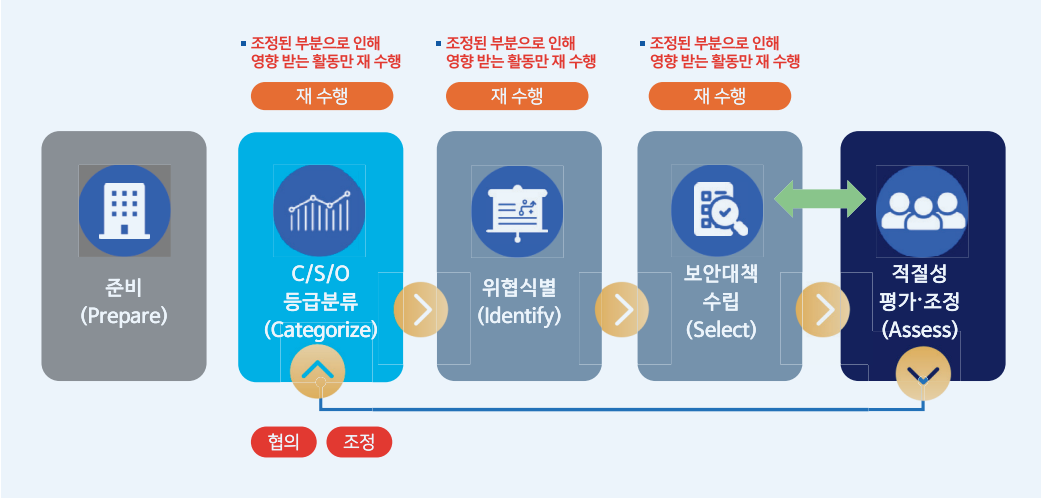
표 3-12 단계별 산출물 목록 및 적절성 평가 항목

구분	주요활동	산출물	내용	비고
준비	NNSF-P-1	▸ N²SF 적용계획	▸ N²SF 단계별 역할/책임 관련 객관성 확보 노력 정도 ▸ 자체 심의위원회 구성 적절성 ▸ 보안요구사항 수립 여부 및 근거 ▸ 수립된 보안요구사항에 대한 N²SF 기본 보안통제 기준선 대비 검토 내역	
	NNSF-P-2	▸ 기관 업무(기능) 목록	▸ 업무(기능) 목록이 기관의 실제 업무를 반영하는지 여부	
	NNSF-P-3	▸ 업무정보 목록	▸ 기관의 기능분류체계(BRM)를 활용한 업무정보의 적절성 여부 ▸ 기관 업무(기능)와 매핑 여부	
	NNSF-P-4	▸ 정보시스템 목록	▸ 업무정보 생명주기 전체 과정이 정보시스템과 함께 식별되었는지 여부 ▸ 정보시스템상에서 업무정보가 다뤄지는 형상, 방식 등 식별 여부	
	NNSF-P-5	▸ 정보서비스 구성	▸ 정보서비스를 구성하는 모든 정보시스템이 식별되었는지 여부	
C/S/O 등급분류	NNSF-C-1	▸ 업무정보C/S/O 목록	▸ 업무정보에 대한 C/S/O 분류 및 근거 적절성 여부 ▸ 업무정보에 대한 과도한 상위등급 분류 여부 ▸ 업무정보에 대한 과도한 하위등급 분류 여부	
	NNSF-C-2	▸ 정보시스템C/S/O 목록	▸ 정보시스템에 대한 C/S/O 분류 및 근거 적절성 여부 ▸ 정보시스템에 대한 과도한 상위등급 분류 여부 ▸ 정보시스템에 대한 과도한 하위등급 분류 여부	
위협식별	NNSF-I-1	▸ 정보서비스 구성(보안등급 포함) 및 서비스·기능	▸ 정보서비스 구성요소 식별 정확성 ▸ 구성요소별 C/S/O 등급 파악 정확성	
	NNSF-I-2	▸「위치-주체-객체」 모델 C/S/O 평가결과	▸ 정보서비스의 기능·유스케이스에 따른 위치-주체-객체 판단 적절성 ▸ 모델 C/S/O 평가 적절성	
	NNSF-I-3	▸「정보 생산·저장」 및 「정보 이동」 위협	▸「정보 생산·저장」 보안원칙 적용 적절성 ▸「정보 이동」 보안원칙 적용 적절성 ▸ 식별된 위협 및 보안대책 적용지점 판단의 적절성	
보안대책 수립	NNSF-S-1	▸ 보안통제 선택 목록	▸ 등급별 보안통제 기준선 검토 여부 ▸ 보안통제 항목 선정의 적절성 여부	
	NNSF-S-2	▸ 보안통제 조정 내역	▸ N²SF 적용계획에 따른 조정 근거의 적절성	필요시
	NNSF-S-3	▸ 보안통제 구현계획	▸ 선택된 보안통제 항목의 구현, 도입 등의 계획 적절성	

2. 적절성 평가결과 협의 및 조정 [NNSF-A-2]

단계별 적절성 평가 결과, 문제점 또는 부적절한 활동이 발견되는 경우 해당 활동이 포함된 단계와 그 이후 단계의 활동을 재수행해야 한다. 단, 조정된 부분으로 인해 영향받는 활동만 재수행 하도록 그 범위를 제한하여 조정에 따른 업무 부담을 경감시킨다.

그림 3-20 조정 대상 단계에 따른 절차별 활동 재수행 개념 및 범위(C/S/O 등급분류 조정 예시)



3. 적절성 평가결과 승인 [NNSF-A-3]

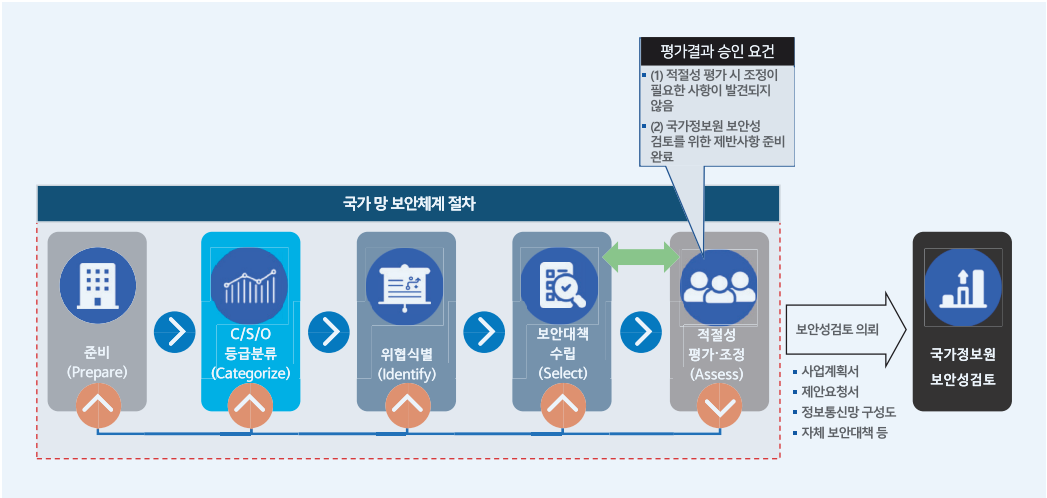
적절성 평가 및 협의·조정이 완료된 후, 적절성 평가결과에 대한 최종 승인은 자체 심의위원회(준비 단계에서 사전 구성)가 심의·의결하며, 적절성 평가결과 승인은 다음 두 가지 조건을 모두 만족하는 경우에만 가능하다.

첫째, 단계별 적절성 평가 시 조정이 필요한 사항이 발견되지 않아야 한다.

둘째, 국가정보원 보안성 검토 의뢰에 필요한 제반사항이 모두 준비되어야 한다.

이를 통해, 국가 망 보안체계의 마지막 활동인 적절성 평가결과 승인을 국가정보원 보안성 검토와 연계되도록 한다.

그림 3-21 적절성 평가결과 승인 요건




국가 망 보안체계
보안 가이드라인

참고

제1절 국가 망 보안체계 기반 제로트러스트 적용 방법

제2절 주요국 보안정책 동향

제3절 접근통제 모델 관점에서 바라본 국가 망 보안체계

제1절

국가 망 보안체계 기반 제로트러스트 적용 방법

국가 망 보안체계의 보안통제 항목은 NIST RMF가 제공하는 오버레이(Overlay) 개념을 적용할 수 있다. 따라서 제로트러스트, 공급망 보안, 회복력 등을 위한 오버레이를 위험관리 활동에 적용할 수 있다. 그렇게 되면, 범용적인 보안통제 항목을 제로트러스트, 공급망 보안, 회복력 관점에서 특화된 내용으로 설계하고 구현할 수 있게 된다.

다음은 미국 국방성(DoD)의 제로트러스트 오버레이를 나타낸다. 이를 이용하면 보안통제 항목에 대해서 제로트러스트 관점의 기능성을 판단할 수 있으며, 결과적으로 조직은 제로트러스트 보안목표 달성을 위해 특정 보안통제 항목을 추가하거나 제로트러스트 기능성 강화를 위해 보안통제 항목의 세부사항을 조정할 수 있다.

그림 참고-1 **보안통제 항목에 대한 Zero Trust 오버레이**

Applicable Controls		Pillars/Enablers							
		Enabler	User	Device	Application & Workload	Data	Network & Environment	Automation & Orchestration	Visibility & Analytics
PT-1	Policy and Procedures	X							
PT-2	Authority to Process Personally Identifiable Information					X		X	
PT-2(1)	Data Tagging					X		X	
PT-2(2)	Automation					X		X	

* 출처: DoD Zero Trust Overlays, June 2024

제2절

주요국 보안정책 동향

1. 영국, GSCP(정부 보안분류 정책)

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

표 참고-1 **영국 GSCP(정부 보안분류 정책) 개요**

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

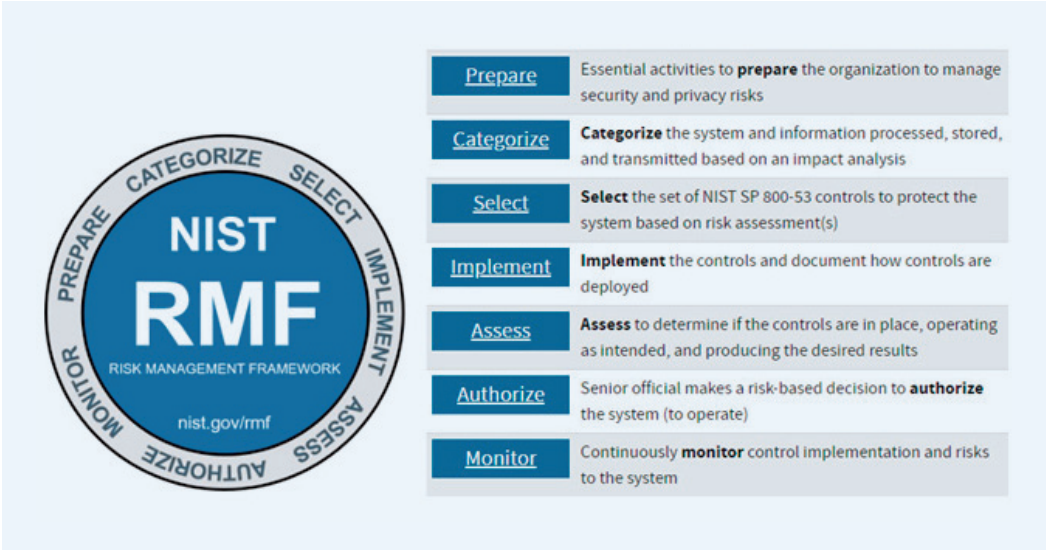
* 출처: 영국정부 웹사이트 gov.uk

TOP SECRET, SECRET, OFFICIAL의 등급으로 정보를 분류하고 등급별로 서로 다른 수준의 보안 요구사항이 적용된다.

2. 미국, NIST RMF

NIST RMF는 미국 연방정보보안현대화법(FISMA)[5]의 요구사항을 충족하며 모든 조직이 정보보안 및 개인정보보호에서 위험을 관리하는 데 사용할 수 있는 포괄적이고 유연한 위험관리 프레임워크이다. NIST RMF는 7단계 절차로 구성되며 지속적인 보안강화를 위해 순환되는 개념을 가지고 있다. 현재는 미국뿐만 아니라 캐나다, 호주, 뉴질랜드, 우리나라 등 많은 국가들이 이를 기반으로 자국의 위험관리 프레임워크를 개발하는 등 정보보안에 관한 위험관리 지침 및 표준으로 받아들여지고 있다.

그림 참고-2 NIST RMF 개요



* 출처: NIST CSRC

NIST RMF는 프레임워크의 전반적인 사항, 위험관리, 위험평가, 보안분류, 보안통제, 지속 모니터링 및 평가 등에 관한 세부적인 지침을 다루는 여러 개의 관련문서로 구성된다.

5 미국의 연방정보보안관리법(FISMA 2002)은 2002년 전자정부법(E-Government Act)의 일환으로 제정되었으며 연방기관의 정보 및 정보시스템에 관한 개발, 문서화, 구현에 관한 요구사항을 다루고 있다. 이후 2014년에 연방정보보안현대화법(FISMA 2014)으로 확대 개정되었으며 연방기관의 보안 요구사항의 근간을 이루고 있다.

3. 캐나다, ITSG-33(IT Security Risk Management)

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

표 참고-2 캐나다 ITSG-33 연혁

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

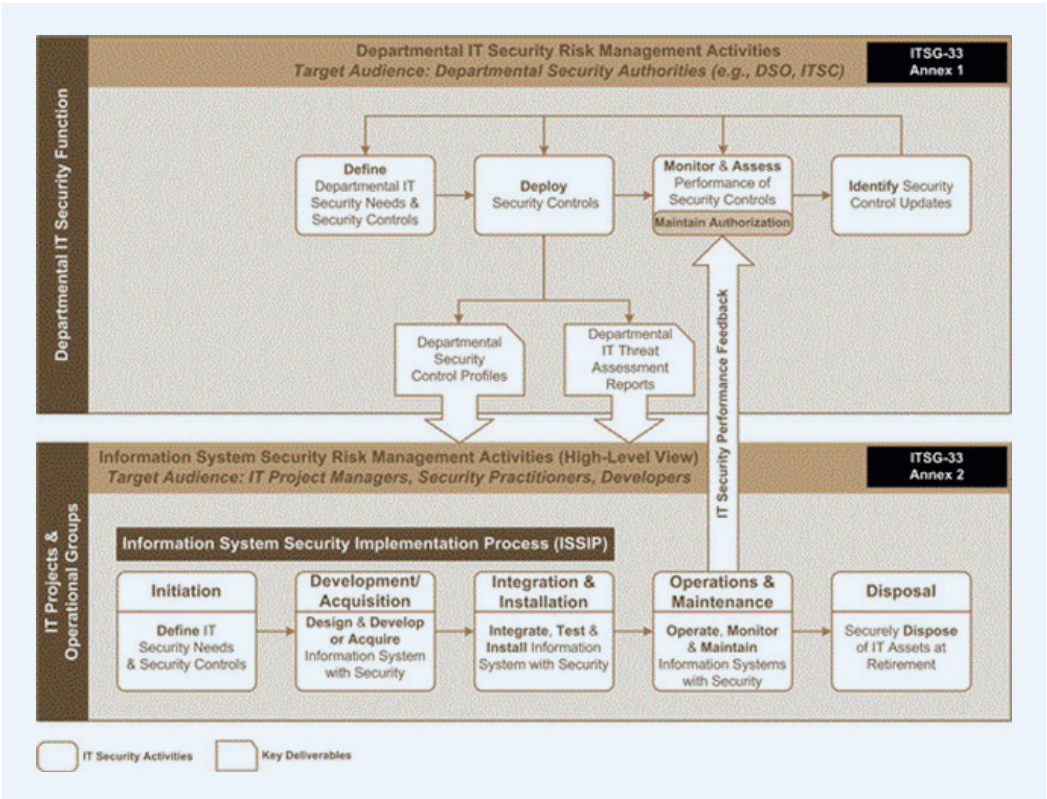
ITSG-33은 위험관리 활동을 크게 ①부서 IT 보안 위험관리 계층과 ②정보시스템 보안 위험관리 계층으로 나누고, 두 개의 상·하위 계층을 유기적으로 연계한다.

①부서 IT 보안 위험관리 계층은 해당 부서의 보안관리자를 위한 것으로, 부서 차원의 보안요구사항과 보안통제를 정의하고 적용하며, 하위계층(②정보시스템 보안 위험관리)과 연계해 보안통제의 효과와 성능을 지속적으로 모니터링 및 평가하여 보안통제를 향상시키는 순환구조로 동작한다.

②정보시스템 보안 위험관리 계층은 IT 프로젝트 매니저, 개발자 및 보안 실무자를 위한 것으로 상위계층(①부서 IT 보안 위험관리)에서 정의된 보안통제의 구현에 중점을 둔다. 기술적 수준의

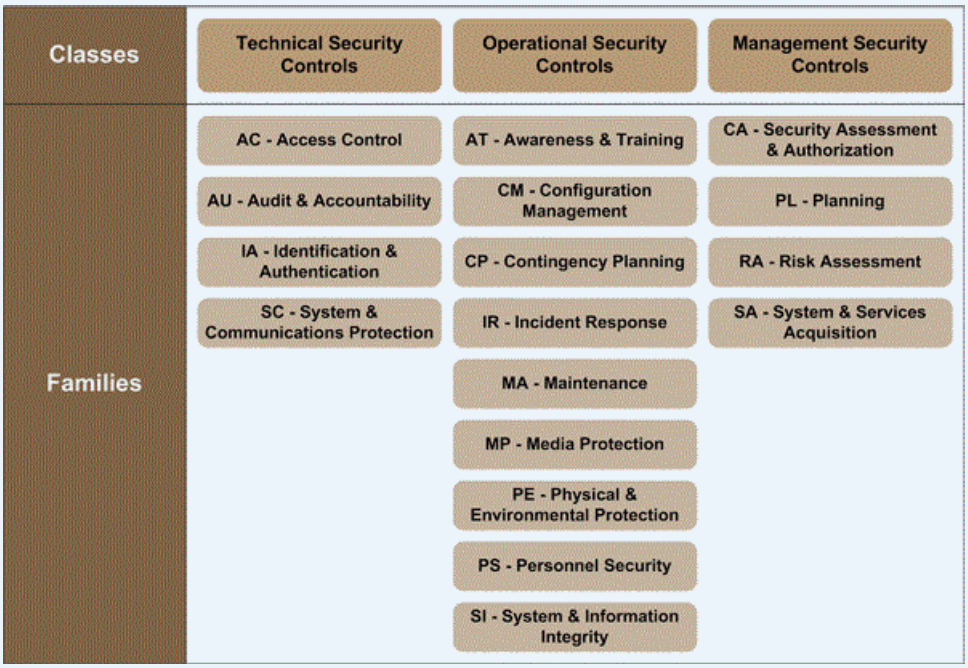
보안요구사항과 보안통제를 정의하고 개발 또는 획득(보안제품 도입 등)을 통해 보안통제를 구현한 후 통합, 설치, 운영, 유지관리를 수행한다. 이 과정에서 보안통제의 효과와 성능에 관한 피드백을 상위계층(①부서 IT 보안 위험관리)과 전달한다.

그림 참고-3 캐나다 ITSG-33 위험관리 계층 구조



ITSG-33의 보안통제는 NIST RMF의 보안통제를 기반으로 하며, 보안통제 패밀리를 기술, 운영, 관리 등 3개의 클래스(Class)로 분류하고 있는 것이 특징이다. 기술(Technical) 클래스는 정보시스템의 하드웨어, 소프트웨어, 펌웨어 수준에서 보안 메커니즘으로서 구현되고 실행되는 보안통제를 뜻한다. 운영(Operational) 클래스는 인력에 의해서 수행되는 정보시스템 운영 절차에 관한 보안통제를 다루고, 관리(Management) 클래스는 정보시스템 관리 활동에 관한 보안통제를 포함한다.

그림 참고-4 캐나다 ITSG-33 보안통제 구성



4. 호주, ISM(Information Security Manual) 및 Essential Eight

호주 정부의 ISM(정보보안 매뉴얼)은 ISMS를 기반으로 정부 기관의 정보보안 가이드라인을 제공하며 거버넌스, 식별, 보호, 탐지, 대응의 영역으로 구성된다.

표 참고-3 호주 ISM(정보보안매뉴얼) 구성

구분	원리(Principles)	
Govern (거버넌스) 강력한 사이버보안 문화 정착	Govern-1	‣ CISO의 사이버보안에 관한 식견 및 리더십
	Govern-2	‣ 시스템, 애플리케이션 및 데이터에 대한 위험관리 활동
	Govern-3	‣ 시스템, 애플리케이션 및 데이터에 대한 보안위험은 운영주기 동안 지속적으로 수용

구분	원리(Principles)	
Identify (식별) 자산 및 자산과 연관된 보안위험 식별	Identify-1	‣ 시스템, 애플리케이션 및 데이터에 대한 임무 중요도 결정 및 문서화
	Identify-2	‣ 시스템, 애플리케이션 및 데이터에 대한 기밀성, 무결성, 가용성 요구사항 결정 및 문서화
	Identify-3	‣ 시스템, 애플리케이션 및 데이터에 대한 보안위험 식별 및 문서화
Protect (보호) 보안위험 관리를 위한 보안통제 구현	Protect-1	‣ 시스템, 애플리케이션의 임무 중요도 및 기밀성, 무결성, 가용성 요구사항에 따른 설계, 배포, 관리
	Protect-2	‣ 신뢰된 공급자에 의한 시스템, 애플리케이션 공급 및 지원
	Protect-3	‣ 공격표면(Attack Surface) 감소를 위한 시스템, 애플리케이션의 설계 및 설정
	Protect-4	‣ 시스템, 애플리케이션 및 데이터에 대한 안전하고 책임추적 가능한 관리
	Protect-5	‣ 시스템, 애플리케이션에 대한 적시적 취약점 식별 및 완화
	Protect-6	‣ 신뢰된 운영체제, 애플리케이션 및 코드만 시스템에서 실행
	Protect-7	‣ 데이터 저장 및 시스템간 이동시 암호화
	Protect-8	‣ 다른 시스템간 데이터 통신에 대한 제어 및 조사
	Protect-9	‣ 애플리케이션, 설정 및 데이터에 대한 안전하고 검증가능한 백업
	Protect-10	‣ 신뢰된 인원만 시스템, 애플리케이션 및 데이터 접근
	Protect-11	‣ 신뢰된 인원의 시스템, 애플리케이션 및 데이터에 대한 최소(업무수행에 필요한 수준)권한 보장
	Protect-12	‣ 시스템, 애플리케이션 및 데이터에 대한 완전하고 안전한 개체 및 접근 관리
	Protect-13	‣ 인원에 대한 지속적인 사이버보안 인식 교육
	Protect-14	‣ 시스템, 관련 인프라 및 시설에 대한 물리적 접근은 승인된 인원으로만 제한
Detect (탐지) 사이버보안 이벤트에 대한 탐지 및 분석을 통한 사고 식별	Detect-1	‣ 사이버보안 사고를 탐지하기 위한 적시적인 이벤트 로그 수집 및 분석
	Detect-2	‣ 사이버보안 이벤트를 통해 사고를 식별하기 위한 적시적인 분석
Respond(대응) 사이버보안 사고 대응 및 복구	Respond-1	‣ 사이버보안 사고에 대한 적시적인 내부 보고 및 외부 보고
	Respond-2	‣ 사이버보안 사고에 대한 적시적인 분석, 격리, 근절, 복구
	Respond-3	‣ 사고대응, 사업연속성 및 재해복구에 관한 계획은 사이버보안 사고로부터 정상적인 임무운영 복구 지원

Essential Eight은 ACSC(호주 사이버보안센터)가 사이버보안 사고감소 전략의 일환으로 사이버공격으로부터 네트워크를 보호하기 위해 실행해야 할 8가지 기본적인 보안조치를 명시한다. 주로 예방적인 조치를 강조하며 비교적 간단하게 측정하고 구현할 수 있는 조치들로 구성된다.

Essential Eight에 포함된 세부전략에는 응용프로그램 보안패치, 운영체제 보안패치, 멀티팩터 인증, 관리자 권한 제한, 응용프로그램 제어, MS Office 매크로 제한, 어플리케이션 하드닝(Hardening), 백업 등이 있다.

그림 참고-5 호주 ACSC의 Essential Eight의 보안통제 영역

호주 정부의 Essential Eight은 기본적인 보안조치에 초점을 맞추고 있어 NIST RMF와 같은 위험관리 프레임워크로 보기에는 무리가 있다. 단, Essential Eight에 다루는 8가지 세부전략은 NIST RMF 보안통제 항목의 일부와 밀접한 관련성이 있다.

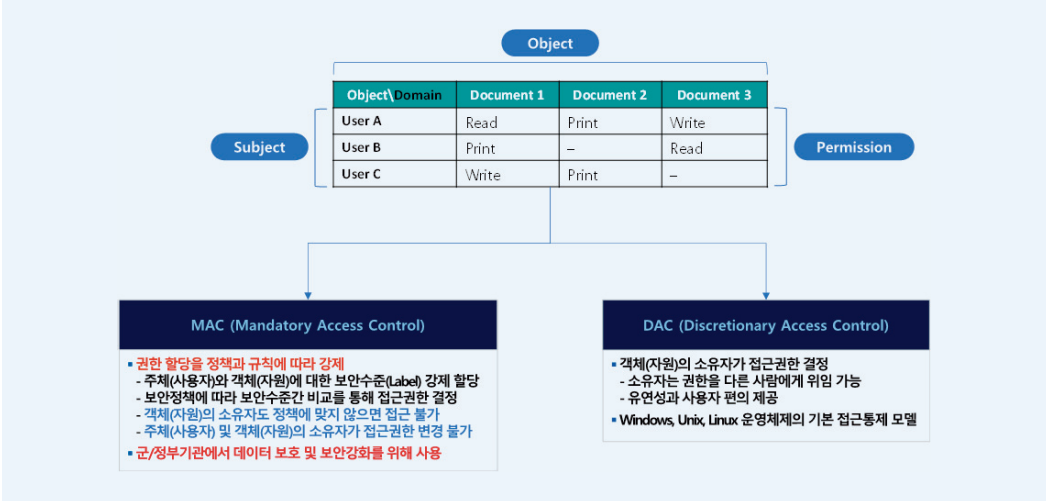
제3절

접근통제 모델 관점에서 바라본 국가 망 보안체계

접근통제(Access Control) 모델은 정보시스템에서 누가(사용자 또는 주체) 무엇(객체)에 접근할 수 있는지를 정의하고, 이를 관리하는 방법을 제공하는 구조적 모델이다. 접근통제 모델은 기밀성, 무결성, 가용성을 보장하기 위해 자원에 대한 접근권한을 설정하고 이를 제한 하는데 사용되며, 보안 요구사항과 환경에 따라 설계된 고유한 접근방식을 제공하는 다양한 접근통제 모델이 있다.

강제적 접근통제(MAC: Mandatory Access Control) 모델은 권한의 할당을 정책과 규칙에 따라 강제하며 각 자원은 보안 레벨이 부여되고, 사용자에게 등급이 매겨지며, 사용자는 자신의 등급에 맞는 자원만 접근할 수 있다. 이는 매우 엄격한 접근통제 방식으로 기밀성을 중시하는 분야(군, 정부기관 등)에서 주로 사용된다.

그림 참고-6 MAC(강제적 접근통제) 모델과 DAC(임의적 접근통제) 모델 비교



임의적 접근통제(DAC: Discretionary Access Control) 모델은 자원의 소유자가 자원에 대한 접근권한을 결정하는 방식으로 유연성과 사용자 편의성을 제공한다. 이 방식은 윈도우즈, 유닉스,

리눅스 등의 운영체제에서 기본 접근통제 모델로 사용된다.

역할기반 접근통제(RBAC: Role-Based Access Control) 모델은 사용자의 역할(Role)을 기반으로 접근권한을 제어하는 방식이다. 사용자는 특정 역할에 할당되며, 각 역할은 고유한 접근권한을 갖는다. 조직구조와 직무에 따라 권한을 부여할 수 있다. 예를 들어, 다음 그림과 같이 Doctor(의사)는 Medicine Record(진료기록)에 Read(읽기) 및 Write(쓰기) 권한을 갖지만, Nurse(간호사)는 Read(읽기) 권한만 갖는다.

속성기반 접근통제(ABAC: Attribute-Based Access Control) 모델은 시간, 시스템 유형, 장소 등의 속성(Attribute)을 기반으로 접근권한을 결정한다. 다양한 조건과 상황을 반영하여 세밀한 접근통제가 가능하다.

예를 들어, 다음 그림과 같이 Time(시각)을 속성으로 설정하여 Employee(일반직원)는 오전 9시부터 오후 5시까지만 컴퓨터를 사용할 수 있고 HR(인사팀직원)은 시간에 제약없이 컴퓨터를 사용할 수 있도록 접근통제가 가능하다.

그림 참고-7 RBAC(역할기반 접근통제) 모델과 ABAC(속성기반 접근통제) 모델 비교

Object\Domain	Patient Information	Medicine Record	Appointment
Doctor	Read write	Read Write	Read Write
Nurse	Read Write	Read	Read
Receptionist	Read Write	–	Read Write

RBAC (Role-based Access Control)

- 사용자의 역할을 기반으로 접근권한 제어
  - 사용자의 역할(role) 정의
  - 각 역할에 수행할 수 있는 작업에 대한 권한 결정
  - 사용자는 하나 이상의 역할을 가질 수 있음

Subject	Attribute: Time	Object: Office Computer	Object: Files
HR	24/7	Access	Access
Team lead	9 am-5 pm	Access	Access
Employee	9 am-5 pm	Access	No access

ABAC (Attribute-based Access Control)

- 속성(Attribute)과 주체/객체/환경에 관한 정책에 따라 접근권한 결정
  - 속성은 역할(role), 자원, 시간, 시스템유형, 장소 등을 포함

국가 망 보안체계(N^2SF)는 기본적으로 MAC(강제적 접근통제)과 같은 강력한 접근통제의 성격을 가지나, MAC 개념에서는 허용하지 않는 정보의 흐름(이동)에 대해서 특정한 속성(요구되는 수준의 보안대책을 적용)을 만족하는 경우에는 제한적으로 허용하고 있다.

따라서, 국가 망 보안체계(N^2SF)는 MAC의 기밀성 중시 및 등급에 따른 강제적 접근통제와 ABAC의 속성(Attribute)에 기반한 특징이 결합된 접근통제 모델로 볼 수 있다.

용어 및 약어

보안 기술 관련 용어

ABAC (Attribute-Based Access Control)	▸ 속성 기반 접근 제어 모델로, 속성 정보(사용자의 속성, 장치 정보, 위치 정보)를 사용하여 접근 제어 관리하는 보안 모델 ▸ 예를 들어, 사용자가 접근하려는 리소스의 위치나 사용자가 접속하는 기기 등의 속성에 따라 접근을 허용하거나 거부 가능
BAS	▸ Breach and Attack Simulation으로 특정 공격기법이나 공격 시나리오를 재연하는 시스템
DAC	▸ 임의적 접근통제 모델은 자원의 소유자가 자원에 대한 접근권한을 결정하는 방식으로 유연성과 사용자 편의성을 제공 ▸ 이 방식은 윈도우즈, 유닉스, 리눅스 등의 운영체제에서 기본 접근통제 모델로 사용
High Water Mark	▸ High Water Mark는 수위가 가장 높이 상승한 지점을 뜻하는 것으로 주로 홍수예방 등의 목적에 사용되는 개념 ▸ 정보보안에서는 정보시스템의 잠재적 보안 영향(Impact)을 평가할 때 보안에 영향을 미치는 여러 가지 요소(예: 기밀성, 무결성, 가용성 등) 중에서 가장 높은 수준의 영향도 값을 해당 정보시스템의 보안 영향도로 인정하는 방법 ▸ 참고: FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, 2004, NIST 및 Wikipedia
MAC	▸ 강제적 접근통제 모델은 권한의 할당을 정책과 규칙에 따라 강제하며 각 자원은 보안 레벨이 부여되고, 사용자에게 등급이 매겨지며, 사용자는 자신의 등급에 맞는 자원만 접근 가능 ▸ 매우 엄격한 접근통제 방식으로 기밀성을 중시하는 분야(군, 정부기관 등)에서 주로 사용
N²SF (National Network Security Framework)	▸ 업무 중요도에 따라 C/S/O 보안등급으로 분류하고 차등적인 보안통제를 적용하는 국내 공공분야 보안정책
RBAC (Role-Based Access Control)	▸ 역할기반 접근통제 모델은 사용자의 역할(Role)을 기반으로 접근권한을 제어하는 방식 ▸ 사용자는 특정 역할에 할당되며, 각 역할은 고유한 접근권한을 가짐 ▸ 조직구조와 직무에 따라 권한을 부여할 수 있음

RMF	▸ 기관(조직) 차원의 다양한 위험(非 사이버위험 포함)을 관리하기 위한 규칙 및 업무 프로세스
보안통제 조정 (Tailoring)	▸ 보안통제 기준선(Baseline)에 따라 기본 선택된 보안통제 항목들에 대해서 수정, 추가, 삭제 등 변경을 가하는 것 ▸ 단, 이러한 조정은 기관이 수립한 NNSF 적용계획, 보안요구사항, 보안통제 조정기준 등에 따름
보안통제 기준선 (Baseline)	▸ 데이터 및 시스템에 대한 보안등급에 따른 기본 보안통제 항목을 선택하기 위한 기준
보안통제 프로파일 (Profile)	▸ 특정 시스템 및 서비스에 대한 보안통제 항목 적용에 관한 세부사항을 정의한 것
보안통제 (Security Control)	▸ 위험을 제거하거나 수용 가능한 수준으로 경감시킬 수 있는 보안대책으로 기술적, 관리적, 운영적 보안통제 등으로 구분됨
오버레이 (Overlay)	▸ 보안통제 항목의 조정에 관한 세부지침 및 보안통제 항목의 구현에 관한 세부사항(Parameter)을 지정한 것 ▸ 제로트러스트(Zero Trust), 공급망보안(Supply Chain Security), 회복력(Resilience) 등에 관한 보안대책을 중점적으로 적용하고자 하는 보안목표를 가지고 있다면, 오버레이(Overlay)를 적용하여 보안통제 항목의 선택, 조정, 구현 과정에서 조직이 목표로 하는 방향성을 반영 가능
위험 (Risk)	▸ 다양한 형태·수준의 위협이 보안대책을 우회하여 기관(조직)에 기술적·운영적 수준의 영향을 끼치는 상태
위협 (Threat)	▸ 기관(조직)에 대한 위험으로 발전할 가능성이 있는 악의적, 비악의적인 의도 또는 현상
유스케이스 (Use Case)	▸ 특정 업무정보 및 정보시스템에 대한 활용 사례, 시나리오 등
제로트러스트 (Zero Trust)	▸ “Never Trust, Always Verify” 철학으로 인증체계 강화, 마이크로 세그멘테이션, 소프트웨어 정의 경계 등의 3가지 핵심원칙을 적용한 보안모델

약어

- **ABAC** Attribute-Based Access Control
- **ACSC** Australian Cyber Security Centre (호주)
- **BAS** Breach and Attack Simulation
- **BRM** Business Reference Model (기능분류체계)
- **CTI** Cyber Threat Intelligence (사이버위협인텔리전스)
- **DAC** Discretionary Access Control
- **DREAD** Damage, Reproducibility, Exploitability, Affected Users, Discoverability
- **FISMA** Federal Information System Modernization Act (미국)
- **GSCP** Government Security Classification Policy (영국)
- **ISM** Information Security Manual (호주)
- **ISMS** Information Security Management System
- **MAC** Mandatory Access Control
- **NIST** National Institute of Standards and Technology (미국)
- **NNSF** National Network Security Framework (국가 망 보안체계)
- **OECD** Organization for Economic Cooperation and Development (경제협력개발기구)
- **OWASP** The Open Worldwide Application Security Project
- **RBAC** Role-based Access Control
- **RMF** Risk Management Framework (위험관리 프레임워크)
- **STIX** Structured Threat Information eXpression
- **STRIDE** Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
- **TAXII** Trusted Automated eXchange of Intelligence Information
- **TTP** Tactics, Techniques and Procedures

참고 문헌

[1] John Kindervag (Forrester), "No More Chewy Centers: Introducing the Zero Trust Model of Information Security", 2010.9.

[2] ATT&CK, https://attack.mitre.org

[3] Threat Modeling with ATT&CK v1.0.0, https://center-for-threat-informed-defense.github.io/threat-modeling-with-attack/

[4] ACSC, "Essential Eight Maturity Model", 2023. 11.

[5] Information Technology Security Guidance, "IT Security Risk Management: A Lifecycle Approach", ITSG-33, 2012, 11.

[6] NIST Risk Management Framework, https://csrc.nist.gov/projects/risk-management

[7] Government Security Classifications Policy, Cabinet Office, 2024. 8.

[8] Guidance 1.1 - Working at OFFICIAL, Cabinet Office, 2024. 8.

[9] Guidance 1.2 - Working at SECRET, Cabinet Office, 2024. 8.

[10] Guidance 1.3 - Working at TOP SECRET, Cabinet Office, 2024. 8.

[11] The NIST Cybersecurity Framework (CSF) 2.0, NIST, 2024. 2.

[12] 조은정, "영국「국가사이버전략 2022」의 특징과 시사점", 국가안보전략연구원, 2022. 9.

[13] 국가안보실, 국가 사이버안보 전략, 2024. 2.

[14] Department of Defense Zero Trust Overlays, Version 1.1, 20204. 6.

[15] NIST Cybersecurity Framework 2.0: Resource & Overview Guide, 2024. 2.

[16] NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

[17] NIST SP 800-30, Rev. 1, Guide for Conducting Risk Assessments

[18] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View

[19] NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations

[20] NIST SP 800-53B, Rev. 5, Control Baselines for Information Systems and Organizations

[21] ISO/IEC 27005:2018, Information technology - Security techniques - Information security risk management

[22] ISO 31000:2018, Risk Management - Guidelines.

[23] ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements

[24] OWASP, Threat Modeling Process, https://owasp.org/www-community/Threat_Modeling_Process

국가 망 보안체계
보안 가이드라인