1.0

국가 망 보안체계
보안 가이드라인

2025. 9





국가정보원 NSR 국가보안기술연구소

1.0

국가 망 보안체계
보안 가이드라인

2025. 9



국가정보원 NSR 국가보안기술연구소

국가 망 보안체계
보안 가이드라인

문서이력

개정일	버전	내역	비고
2025.1.	Draft	「국가 망 보안체계 보안 가이드라인」 Draft 발간	
2025.9.	1.0	「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 보안 프레임워크이다.

각급기관은 국가 망 보안체계 도입을 위한 신규 정보화사업 계획·시행 시 본 가이드라인에 따라 자율적으로 위협을 식별한 후, 그에 대한 보안대책을 수립하여 보안통제를 선정하고 구현·운영할 수 있다. 이를 위해 국가 망 보안체계의 보안통제 항목과 C/S/O 보안등급별 우선 검토사항을 제공한다.

또한, 국가 망 보안체계를 적용하여 변화되는 공공부문의 정보서비스 환경을 구체적인 예시로 설명한 주요 정보서비스 모델을 제시한다. 각 정보서비스 모델은 산·학·연·관 전문가들이 위협식별, 보안 요구사항 도출, 관련 규정·지침·보안 가이드라인 분석 등의 과정을 거쳐 수립한 보안통제 항목을 함께 제공한다.

각급기관은 정보서비스 모델을 참조하여 업무환경의 AI·클라우드 등 신기술 활용이 가능한 국가 망 보안체계로의 전환을 추진할 수 있다.

각급기관은 본 가이드라인 외에 추진하고자 하는 정보서비스의 구성 및 특성에 따라 보안통제 항목 적용·구현 시 관련 법령·지침[1], 보안 가이드라인[2] 등을 준용한다.

2. 문서의 구조와 기술 범위

1장은 국가 망 보안체계의 추진배경, 개념, 적용절차, 기본원칙, 고려사항 등을 소개한다.

2장은 국가 망 보안체계를 국가·공공기관에 적용하는 절차와 주요활동에 관한 세부내용, 적용·운용 시의 참고사항 등을 설명한다. 특히, 국가·공공기관이 자율적으로 정보서비스에 대한 위협을 식별하고, 그에 대한 보안대책을 수립하여 보안통제를 선정하는 방법 등을 제시한다.

3장은 국가 망 보안체계의 각 단계별 주요활동을 요약하고 국가정보원 보안성 검토 시 제출하는 문서의 형식을 정의한다.

---

1) 「국가정보보안기본지침」 등

2) 「국가 클라우드 컴퓨팅 보안 가이드라인」, 「챗GPT 등 생성형 AI 활용 보안 가이드라인」 등

CONTENTS

제1장 국가 망 보안체계(N2SF)

제1절 추진배경 ····· 10
제2절 국가 망 보안체계 개요 ····· 13
제3절 국가 망 보안체계 핵심 개념 ····· 20
제4절 고려사항 ····· 28

제2장 국가 망 보안체계(N2SF) 적용 절차

제1절 준비(Prepare) ····· 33
제2절 C/S/O 등급분류(Categorize) ····· 40
제3절 위협식별(Identify) ····· 44
제4절 보안대책 수립(Select) ····· 50
제5절 적절성 평가·조정(Assess) ····· 55

제3장 산출물 및 보안성 검토

제1절 단계별 주요활동 요약 ····· 64
제2절 보안성 검토 시 제출하는 최종 산출물 ····· 66

참고

제1절 주요국 보안정책 동향 ····· 72
제2절 N2SF 오버레이 개념을 통한 절차·원칙 통합 보안체계 ····· 77
제3절 CDS(Cross Domain Solution) ····· 79

■ 주요 용어 및 약어 ····· 81
■ 참고문헌 ····· 85

Table List

〈표 1-1〉 보안통제 항목의 구조 [예: 원격접속(Remote Access, RA)] ····· 27
〈표 2-1〉 국가 망 보안체계 단계별 주요활동(요약) ····· 32
〈표 2-2〉 준비(Prepare) 단계 주요활동별 수행내용 ····· 33
〈표 2-3〉 N2SF 적용계획 수립[활동-1-1]의 세부활동 ····· 35
〈표 2-4〉 업무정보 식별 예시 ····· 37
〈표 2-5〉 정보서비스 사용 시나리오 정의 예시 ····· 39
〈표 2-6〉 정보서비스 보안목표 설정 예시 ····· 39
〈표 2-7〉 C/S/O 등급분류 단계 주요활동별 수행내용 ····· 40
〈표 2-8〉 업무정보에 대한 C/S/O 등급분류 기준 ····· 41
〈표 2-9〉 정보시스템에 대한 C/S/O 등급분류 예시 및 주의사항 ····· 43
〈표 2-10〉 위협식별(Identify) 단계 주요활동별 수행내용 ····· 44
〈표 2-11〉 보안대책 수립(Select) 단계 주요활동별 수행내용 ····· 50
〈표 2-12〉 보안통제 구현계획 수립의 세부 활동 ····· 54
〈표 2-13〉 적절성 평가·조정(Assess) 단계 주요활동별 수행내용 ····· 56
〈표 2-14〉 준비(Prepare) 단계에 대한 적절성 평가지표 ····· 56
〈표 2-15〉 C/S/O 등급분류(Categorize) 단계에 대한 적절성 평가지표 ····· 57
〈표 2-16〉 위협식별(Identify) 단계에 대한 적절성 평가지표 ····· 58
〈표 2-17〉 보안대책 수립(Select) 단계에 대한 적절성 평가지표 ····· 58
〈표 3-1〉 단계별 주요활동 요약 ····· 64
〈표 3-2〉 국가 망 보안체계 수행결과를 이용한 보안성 검토 ····· 66
〈표 참고-1〉 영국 GSCP(Government Security Classifications Policy) 개요 ····· 74
〈표 참고-2〉 캐나다 ITSG-33 연혁 ····· 74
〈표 참고-3〉 호주 ISM(정보보안매뉴얼) 구조 ····· 76

CONTENTS

Figure List

[그림 1-1] 망 분리 정책 개선 추진경과 ····· 11

[그림 1-2] 망 분리 정책 개선 추진 목표 ····· 12

[그림 1-3] 기존 망 분리 정책과 국가 망 보안체계 비교 ····· 14

[그림 1-4] 국가 망 보안체계 적용 절차 ····· 14

[그림 1-5] 단계별 주요활동 구성 및 상관관계 ····· 16

[그림 1-6] 보안목표·보안위협·보안 요구사항·보안통제 상호관계 ····· 18

[그림 1-7] 국가 망 보안체계와 국가·공공기관 정보보안 업무 ····· 19

[그림 1-8] 기능분류체계·기관업무·업무정보·정보시스템·정보서비스의 관계 ····· 21

[그림 1-9] C/S/O 등급분류 절차 ····· 22

[그림 1-10] 업무정보 C/S/O 분류 기준 ····· 23

[그림 1-11] 정보서비스 모델링 개념 ····· 24

[그림 1-12] 정보서비스에 대한 모델 C/S/O 평가 및 보안원칙 적용 ····· 25

[그림 1-13] 보안통제 항목 예시(부록1) ····· 26

[그림 2-1] 준비(Prepare) 단계 주요활동 흐름도 ····· 34

[그림 2-2] 정부기능분류체계 (출처: 국가기록원) ····· 36

[그림 2-3] 정부기능분류체계와 기관 자체 BRM 연계 예시 ····· 36

[그림 2-4] 업무정보 식별 개념도 ····· 37

[그림 2-5] 정보시스템 식별 개념도 ····· 38

[그림 2-6] C/S/O 등급분류(Categorize) 단계 주요활동 흐름도 ····· 40

[그림 2-7] 정보시스템의 C/S/O 등급분류 기준 (좌: 동일 등급의 경우, 우: 복수 등급의 경우) ····· 42

[그림 2-8] 위협식별(Identify) 단계의 주요활동 흐름도 ····· 45

[그림 2-9] 「위치-주체-객체」 모델링 및 C/S/O 평가 개념도 ····· 46

[그림 2-10] 「위치-주체-객체」 모델링 및 C/S/O 평가 예시 (업무환경에서 생성형 AI 활용) ····· 47

[그림 2-11] 「정보 생산·저장」 보안원칙 적용 예시 (업무환경에서 생성형 AI 활용) ····· 48
[그림 2-12] 「정보 이동」 보안원칙 적용 예시 (업무환경에서 생성형 AI 활용) ····· 49
[그림 2-13] 보안대책 수립(Select) 단계의 주요활동 흐름도 ····· 51
[그림 2-14] 국가 망 보안체계 보안통제 항목 선택 방법(예: O등급 업무정보· 정보시스템) 53
[그림 2-15] 적절성 평가조정 개념도 ····· 55
[그림 2-16] 조정 대상 단계에 따른 절차별 활동 재수행 개념 및 범위 (C/S/O 등급분류 조정 예시) ····· 59
[그림 2-17] 적절성 평가결과 확인 요건 ····· 60
[그림 참고-1] NIST RMF를 구성하는 관련문서(가이드라인) 목록 ····· 72
[그림 참고-2] NIST RMF의 위험관리를 위한 각 단계 주요활동 ····· 73
[그림 참고-3] 캐나다 ITSG-33 구조 ····· 75

국가 망 보안체계
보안 가이드라인



제1장

국가 망 보안체계(N2SF)

제1절 추진배경

제2절 국가 망 보안체계 개요

제3절 국가 망 보안체계 핵심 개념

제4절 고려사항

제1절

추진배경

망 분리 정책은 2006년부터 국가·공공기관을 대상으로 시행하였으며 이후 금융 및 방산 등으로 확대되었다. 망 분리 정책의 주 목적은 민감한 데이터를 다루는 내부망(업무망)을 인터넷망과 분리 운영하여 인터넷을 통한 불법적인 접근이나 정보유출 등 외부로부터의 사이버 위협을 원천적으로 차단하는 것이다.

망 분리 정책은 현재까지 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 이유 중의 하나가 바로 망 분리 정책의 효과라는 것이 많은 전문가들의 견해이다.

그동안 IT 환경의 변화와 현장의 애로사항을 반영해 논리적 망 분리, 망연계 등을 적용하여 편의성을 일부 향상시키고 필수적인 데이터의 소통을 허용하는 등 망 분리 정책은 시대적 상황에 따라 유연하게 변화되어 왔다.

그러나 코로나19 이후 재택·원격근무의 도입과 함께 클라우드, 생성형 AI 등 최신 IT 기술을 활용하여 보다 효율적인 업무환경을 구축하려는 요구가 높아졌다. 기존의 망 분리 정책은 이러한 변화에 신중하게 대응하도록 하였으나, 이를 계기로 다양한 업무환경 변화와 신기술 도입에 부합하는 새로운 보안정책 방향에 대한 논의가 본격화되는 계기가 되었다.

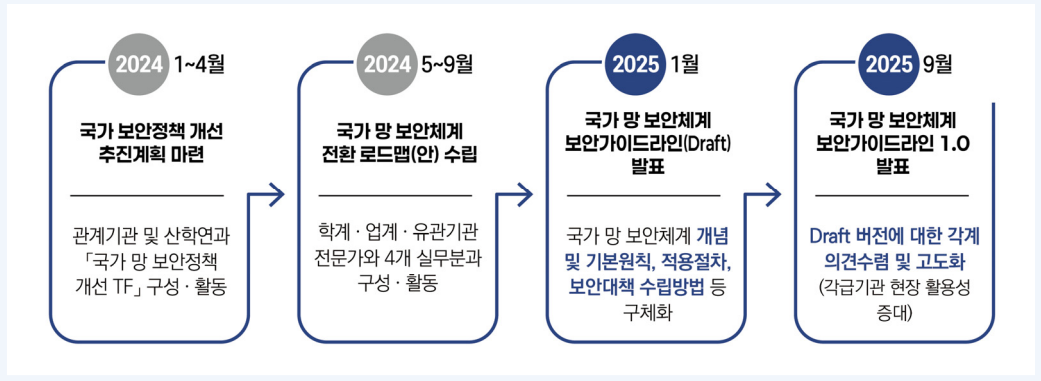
재택근무 등 새로운 업무환경을 반영하고, 신기술 도입을 적극 추진할 수 있도록 망 분리 정책의 발전 방향을 모색하는 움직임이 한층 활발해졌으며, 이를 통해 보안성을 유지하면서도 업무 효율성과 혁신을 동시에 달성할 수 있는 정책적 해법에 대한 기대가 높아졌다.

이에 따라 국가정보원은 관계기관과 산학연 전문가들이 참여하는 「국가 망 보안정책 개선 TF」를 구성하여, 변화된 환경에 부합하는 보안정책 수립에 착수하였다.

TF는 내부 논의와 전문가 자문을 거쳐, 보안성을 확보하면서 공공데이터 활용 활성화와 업무 효율성 제고를 동시에 달성할 수 있는 방향을 마련하였다.

국가정보원은 업무정보의 중요도에 따라 보안통제를 차등 적용하는 '국가 망 보안체계'를 새롭게 수립하였으며, 제도 시행 초기임을 고려하여 2025년 1월 보안 가이드라인 Draft(초안)를 공개하고, 학계·업계·유관기관·각급기관의 의견을 폭넓게 반영하여 현장의 이해도와 활용성을 높인 '보안가이드라인 1.0'을 발표함으로써, 변화된 환경에 부합하는 실효적인 보안정책을 마련하였다.

그림 1-1 망 분리 정책 개선 추진경과



국가 망 보안체계는 다음과 같은 5가지 목표를 중심으로 추진된다.

첫째, 기존의 획일적인 망 분리 방식을 넘어 국가 망 보안체계 기반의 보안정책으로 패러다임을 전환하여 보다 유연하고 효율적인 보안 환경을 조성한다.

둘째, AI·클라우드 등 신기술 융합해 정보유통을 강화함으로써 언제 어디서나 업무를 수행할 수 있는 스마트 업무환경을 실현한다.

셋째, 산·학·연·관 전문가와 협력을 통해 기관 자율보안 개념을 접목하고, 국내 현실에 최적화된 보안정책을 개발한다.

넷째, 새로운 보안정책을 신속하게 제시하여 각 기관이 환경과 여건에 맞게 자율적으로 추진하도록 지원하고, 평가·검증 제도 등 관련 제도를 점진적으로 개선해 안정적으로 안착시킨다.

다섯째, 공공정보의 보안성과 활용성을 동시에 높여 보안기술 및 AI·클라우드·공공데이터 산업 발전을 촉진하고, 디지털 경제 활성화에 기여한다.

그림 1-2 망 분리 정책 개선 추진 목표



제2절

국가 망 보안체계 개요

1. 국가 망 보안체계 도입

세계 주요국들이 AI 인프라 투자에 속도를 내는 가운데, 우리 정부도 AI·클라우드 등 신기술을 글로벌 경쟁력 확보와 기술 주도형 경제로의 전환을 이끌 핵심 성장동력으로 육성하고 있다. 이러한 흐름 속에서 국가·공공기관 역시 신기술을 활용하여 행정업무를 효율성을 높이고, 민·관이 융합된 다양한 서비스를 창출하여 국민이 체감할 수 있는 혁신적인 디지털 공공서비스를 확산 할 필요가 있다.

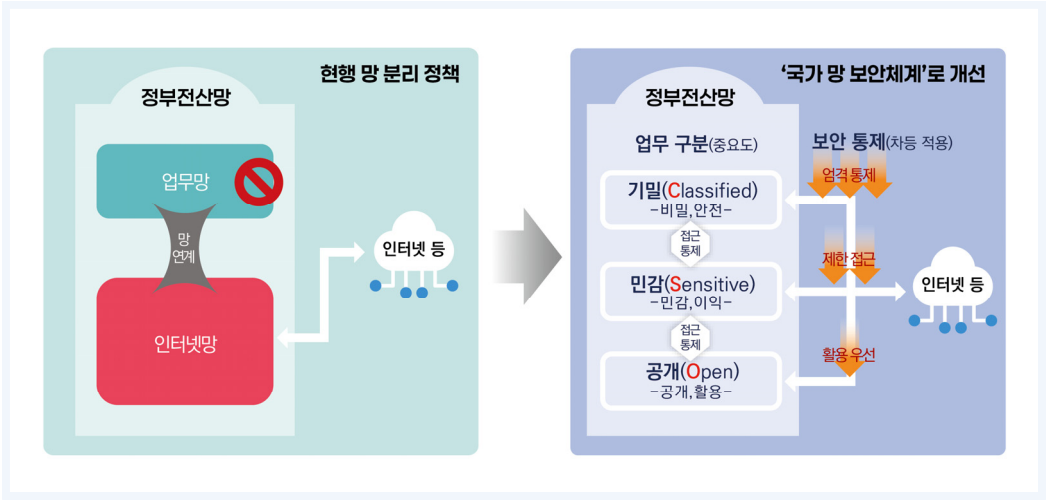
다만, 망 분리 환경을 완화하는 과정에서는 국가 핵심 기능을 수행하는 국방, 외교, 행정, 금융 등 분야의 업무 연속성과 국가안보를 굳건히 지키기 위해 충분하고 체계적인 보안대책을 병행하는 것이 필수적이다.

이에 국가·공공기관은 선제적으로 잠재 위협을 식별하고, 그로 인한 국가기능의 위험을 정확히 평가한 뒤, 적절한 보안대책을 수립·적용함으로써 조직의 업무와 기능을 안정적으로 보호하고 보안태세를 강화해야 한다.

국가 망 보안체계(N2SF)는 각급기관의 업무정보·정보시스템을 식별하고, 업무 중요도에 따라 기밀(Classified), 민감(Sensitive), 공개(Open) 등급으로 분류하여 등급별로 차등적인 보안통제를 적용하는 보안 프레임워크이다.

이 체계는 기본원칙과 세부 절차를 통해 각급기관이 자율적으로 위험을 진단하고 보안대책을 설계·시행할 수 있도록 지원함으로써, 높은 수준의 보안성과 원활한 데이터 활용이라는 두 가지 목표를 동시에 달성하도록 한다.

그림 1-3 기존 망 분리 정책과 국가 망 보안체계 비교



2. 국가 망 보안체계 적용 절차

국가 망 보안체계는 각급기관의 정보화사업에 대한 자체 보안대책을 수립하는 데 활용하며 ❶준비, ❷C/S/O 등급분류, ❸위협식별, ❹보안대책 수립, ❺적절성 평가·조정의 5단계 절차로 수행한다.

그림 1-4 국가 망 보안체계 적용 절차



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

❷C/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.

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

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

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

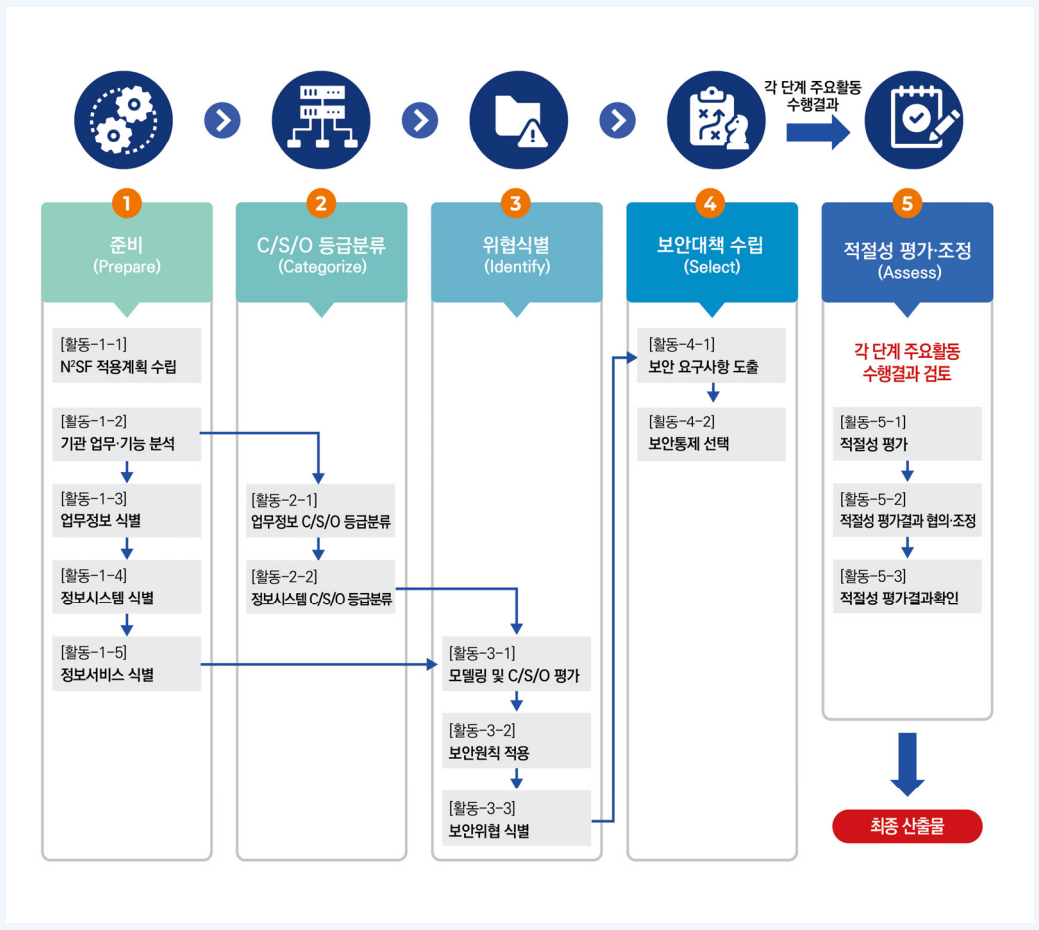
국가 망 보안체계의 모든 단계가 완료되면 절차에 따라 국가정보원에 보안성 검토를 요청한다.

이와 같이 국가·공공기관은 정보화사업(정보서비스 신규 구축 및 기존 운영 중인 정보서비스에 대한 N2SF 적용 포함)을 추진할 때 국가 망 보안체계를 이용하여 표준화된 5단계 절차에 따라 기관이 자율적으로 위협을 식별하고 적절한 보안대책을 수립할 수 있다.

3. 단계별 주요활동 및 상호관계

다음 그림은 단계별 주요활동의 구성 및 관계도이다. 각 활동의 수행결과는 다른 활동에 영향을 미치며, 적절성 평가·조정 단계에서 종합적으로 분석된 후 최종 산출물을 완성한다.

그림 1-5 단계별 주요활동 구성 및 상관관계



첫째, 준비 단계는 국가 망 보안체계 전체 절차를 위한 기초 데이터를 수집하고 N2SF 적용계획을 수립한다.

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, 위협식별 결과에 따라 업무정보, 정보시스템, 네트워크 연계 지점 등에 대한 적절한 보안통제 항목을 선택한다. C/S/O 보안등급별 「우선검토 사항」을 활용해서 보안등급에 따른 필요 보안통제 항목을 선택할 수 있고, 기관의 특성 및 정보서비스 환경을 반영하여 보안통제 항목의 제외·수정·추가 등 조정이 가능하다.

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

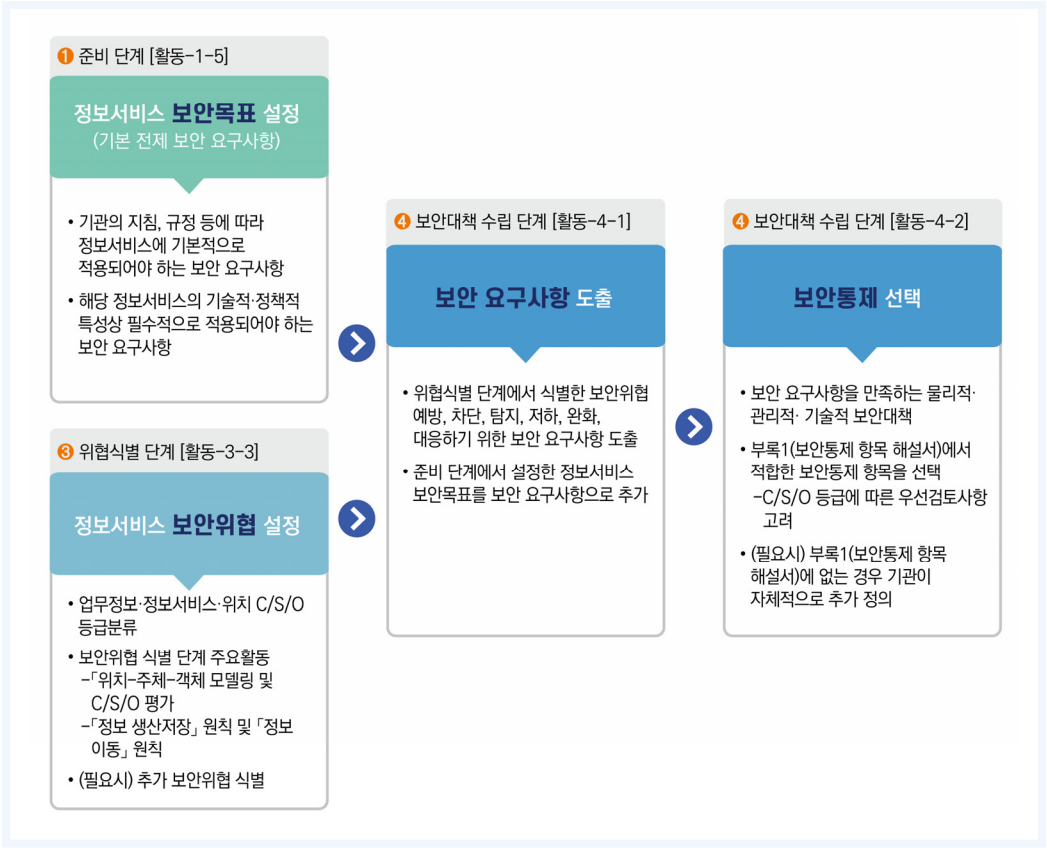
4. 보안 요구사항 수립 및 보안통제 항목 선정

준비 단계에서 정보서비스에 대한 기본적인 보안 요구사항을 보안목표로 설정할 수 있다. 기관의 지침, 규정 등이 해당 정보서비스에 대한 필수적인 보안 요구사항을 포함되는 경우 이를 보안목표로 설정할 수 있다. 또한, 해당 정보서비스의 기술적·정책적 특성상 필수적인 보안 요구사항이 있다면 보안목표에 이를 추가할 수 있다.

위협식별 단계에서 「위치-주체-객체」 모델링 및 C/S/O 평가, 「정보 생산·저장」 원칙, 「정보 이동」 원칙 등을 적용하여 보안위협을 식별한 후, 각 보안위협에 대한 예방·차단·탐지·대응·완화·복구 등이 가능한 보안 요구사항을 수립하게 된다. 이때 앞서 준비 단계에서 수립한 보안목표를 보안 요구사항에 추가하여 정보서비스에 대한 종합적인 보안 요구사항을 수립하게 된다.

이렇게 수립된 보안 요구사항을 만족하는 관리적·물리적·기술적 보안대책으로서 보안통제 항목을 부록1(보안통제 항목 해설서)에서 선택하게 되는데 이때 C/S/O 등급에 따른 우선 검토사항을 고려한다. 만약, 특정 보안 요구사항에 대한 적합한 보안대책이 부록1에 없다면 기관이 자체적으로 보안통제 항목을 추가 정의할 수 있다.

그림 1-6 보안목표·보안위협·보안 요구사항·보안통제 상호관계



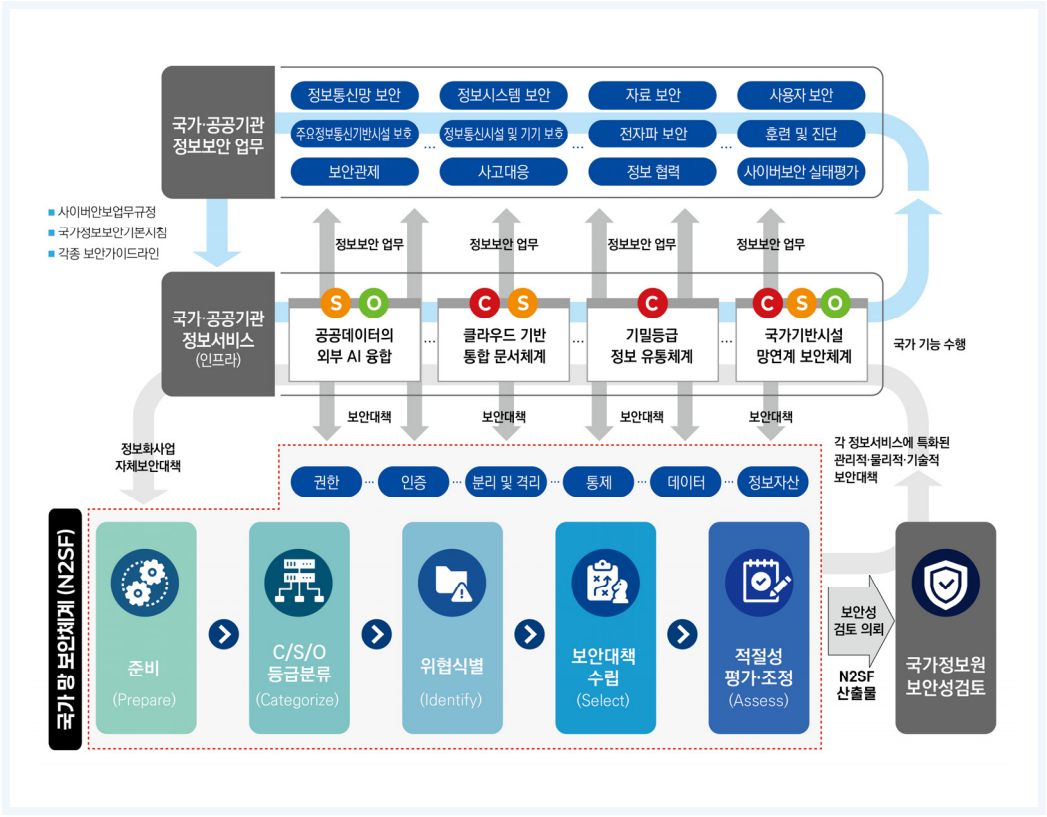
5. 정보보안을 위한 국가 망 보안체계의 중요성

국가·공공기관은 기관별 고유한 국가기능을 수행하며, 이를 위해 다양한 내부 업무 체계와 대국민 서비스를 운영한다. 이러한 기능을 안정적으로 유지하기 위해서는 정보의 유출, 위·변조, 훼손을 예방하는 관리적·물리적·기술적 보안조치가 필수적이다. 국가 망 보안체계는 이러한 보안활동의 중심축으로, 정보서비스 단계에서 발생할 수 있는 보안위협을 사전에 식별·평가하고 선제적으로 대응할 수 있도록 한다.

또한, 정보서비스는 보안관제, 모의훈련, 보안진단, 사이버보안 실태평가 등 다양한 정보보안 업무의 대상이 된다. 국가 망 보안체계에 의해 사전 적용된 보안통제는 이러한 활동의 기반이 되어, 기관이 일관되고 체계적인 보안관리를 수행할 수 있게 한다.

결과적으로 국가 망 보안체계는 보안성 강화와 업무 연속성 보장을 동시에 달성하는 핵심 프레임워크로서, 국가·공공기관의 정보보안 수준을 한 단계 끌어올리는 데 중요한 역할을 한다.

그림 1-7 국가 망 보안체계와 국가·공공기관 정보보안 업무



제3절

국가 망 보안체계 핵심 개념

1. 기능분류체계와 연계한 각급기관의 업무·업무정보 식별

국가 망 보안체계는 정부기능분류체계, 지방기능분류체계 등의 기능분류체계와 연계하여 각급기관의 업무를 식별할 것을 권고한다. 이를 통해 업무정보에 대한 C/S/O 등급분류시 기관의 수행 업무·기능을 기준으로 중요도를 판단하는 기준점을 확보할 수 있다.

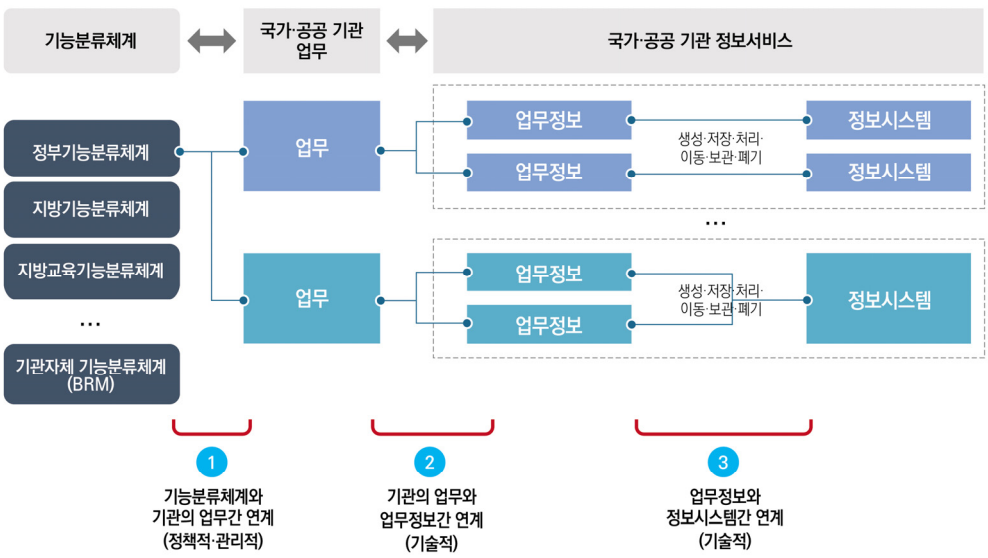
다음 그림은 ❶기능분류체계와 기관의 업무, ❷기관의 업무와 업무정보, ❸업무정보와 정보시스템에 이르는 연계성을 설명하고 있다.

첫째, ❶국가·공공기관 업무를 분류할 때 정부기능분류체계, 지방기능분류체계, 지방교육기능분류체계 등의 기능분류체계를 활용할 수 있다. 즉, 각급기관의 업무정보에 대한 C/S/O 등급분류 및 중요도 등을 판단할 때 큰 틀의 기준으로서 참고·활용할 수 있다.

둘째, ❷각급기관이 업무를 수행할 때 사용되거나 생산되는 업무정보를 식별하여 해당 업무와 업무정보를 연관 지을 수 있다.

셋째, ❸특정 업무정보에 대한 생성·저장·처리·이동·보관·폐기 등에 관여하는 정보시스템을 식별하여 해당 업무정보와 정보시스템을 연관 지을 수 있다. 정보서비스는 1개 이상의 정보시스템으로 구성된다.

그림 1-8 기능분류체계·기관업무·업무정보·정보시스템·정보서비스의 관계



2. 등급분류

가. 등급분류 절차

업무정보, 정보시스템, 위치(물리적·논리적)에 대한 C/S/O 등급분류는 다음 순서로 수행한다.

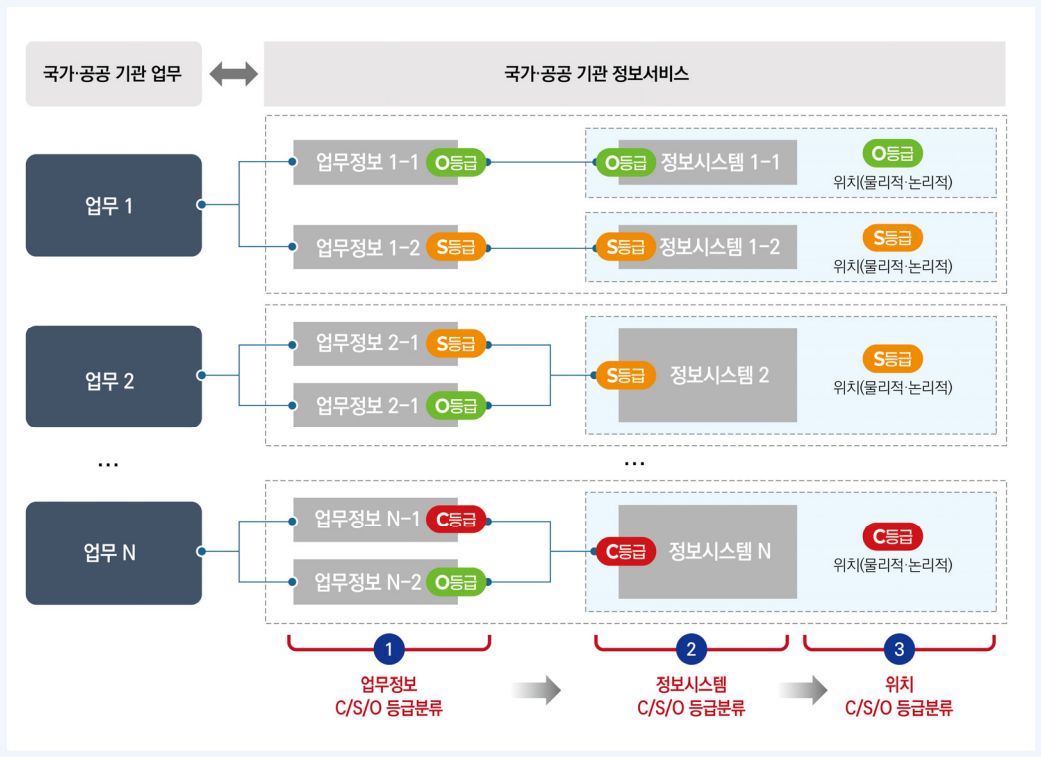
❶ 업무정보 분류 : 각급기관의 업무에 이용되는 업무정보를 C/S/O 등급으로 분류한다.

❷ 정보시스템 분류 : 업무정보의 등급을 기반으로 해당 정보를 처리하는 정보시스템의 C/S/O 등급을 결정한다.

❸ 위치 분류 : 정보시스템의 물리적·논리적 위치에 따라 정보시스템의 C/S/O 등급정보와 연계하여 등급분류를 수행한다.

이 과정에서 공개 가능한 정보가 불필요하게 비공개로 분류되거나, 반대로 비공개 정보가 공개로 분류되지 않도록 주의를 기울여야 한다.

그림 1-9 C/S/O 등급분류 절차



나. 업무정보 C/S/O 등급분류 기준

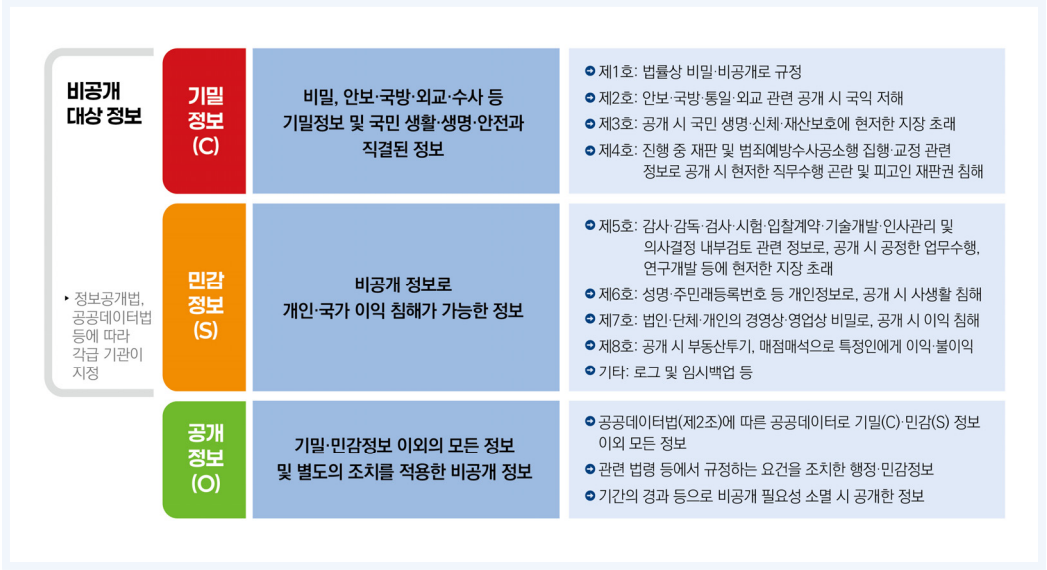
업무정보의 등급분류 기준은 관련 법령에 근거하고 있다. 기밀정보(C등급)와 민감정보(S등급)는 「정보공개법」, 「공공데이터법」, 「보안업무규정」 등에 따라 각급기관이 지정한 비공개 정보에 해당한다.

기밀정보(C)는 비밀, 안보·국방·외교·수사 등의 기밀정보와 국민 생활·생명·안전과 직결된 정보로서 「정보공개법」 제9조(비공개 대상 정보)의 제1호~제4호에 해당한다.

민감정보(S)는 공개 시 개인·국가 이익 침해가 우려되는 정보로서 「정보공개법」 제9조(비공개 대상 정보)의 제5호~제8호에 해당하는 정보 및 시스템 로그, 임시백업 등의 기타 정보를 포함한다.

공개정보(O)는 기밀정보(C) 및 민감정보(S) 이외의 모든 정보가 해당된다. 또한 관련 법령에 규정된 정보 공개 요건을 충족한 비공개 정보와 기간의 경과 등으로 비공개 필요성이 소멸된 정보도 공개정보(O) 등급으로 분류한다.

그림 1-10 업무정보 C/S/O 분류 기준



다. 정보시스템 C/S/O 등급분류 기준

정보시스템의 C/S/O 등급은 기본적으로 해당 정보시스템이 생산·저장·처리하는 업무정보의 C/S/O 등급과 동일하게 분류한다.

다만, 하나의 정보시스템에 서로 다른 등급의 업무정보가 포함되는 경우에는 가장 높은 등급을 해당 정보시스템의 등급으로 분류한다.

이때, 낮은 등급의 업무정보에 대해 높은 등급 수준의 보안대책이 적용되어 공공정보 활용에 제약이 발생할 수 있으므로, 동일 등급별로 정보시스템을 분리·운영할 것을 권고한다.

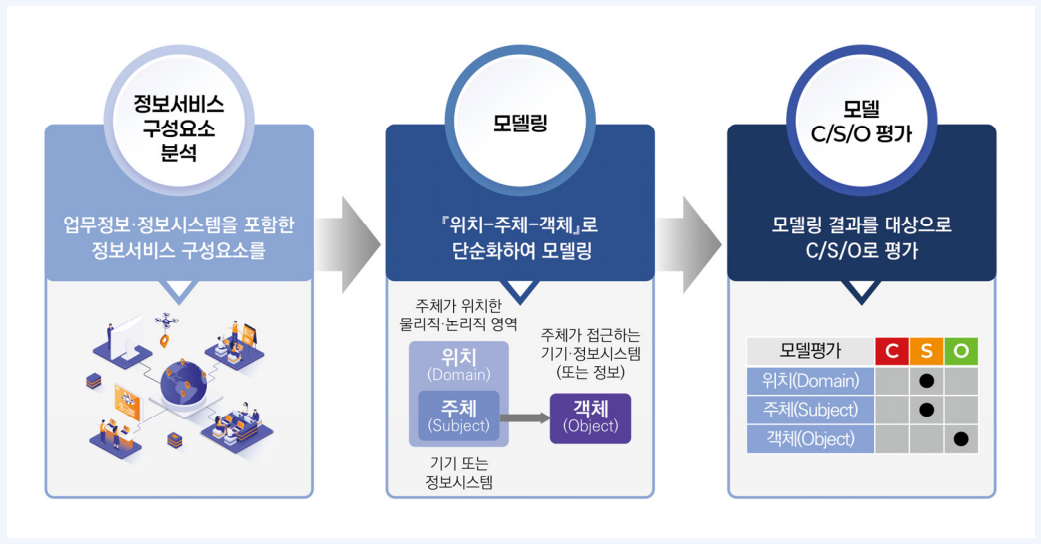
라. 위치 C/S/O 등급분류 기준

정보시스템의 논리적인 위치(영역)에 대해 C/S/O 등급으로 분류한다. 인터넷 영역은 O등급, 업무영역은 S등급, 이외 기밀 등을 취급하기 위한 특수한 환경 등은 C등급으로 분류하는 것이 원칙이다. 위치에 대한 등급 분류가 필요한 이유는 위협식별 및 보안대책 수립 절차에서 기초자료로 활용된다.

3. 위협 모델링과 식별 절차

국가 망 보안체계에서는 정보시스템에서 발생 가능한 구조적 위협을 사전에 식별하고 그에 대한 보안대책을 수립하기 위해 위협 모델링을 수행한다. 위협 모델링은 복잡한 실제 정보서비스 구조에서 핵심 요소만 단순화하여 보안위협을 효과적으로 파악하는 기법이다.

그림 1-11 정보서비스 모델링 개념



먼저, 정보서비스 구성환경을 「위치-주체-객체」로 단순화하여 표현한다. 여기에서 주체(Subject)는 업무정보를 활용하는 정보시스템으로 의미하고, 객체(Object)는 주체가 접속하거나 이용하는 대상 정보시스템을 뜻한다. 위치(Domain)는 주체가 위치한 물리적·논리적 영역을 나타낸다. 각 위치, 주체, 객체에는 C/S/O 보안등급이 부여된다.

「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.

모델링 결과 보안등급의 혼용이 발생하는 경우 보안위협이 존재하며 그에 따른 적절한 보안대책이 요구된다. 예를 들어, 「위치」와 「주체」는 모두 S등급이나 「객체」가 O등급인 경우 「주체」, 「객체」, 「주체와 객체 간 연계구간」 등 3곳에 보안대책 적용을 검토할 필요가 있다.

정보서비스에 대한 「위치-주체-객체」 모델링 및 모델 C/S/O 평가를 수행한 후 서로 다른 보안등급 간 혼용이 발생하는 경우, 구체적으로 어떤 업무정보와 정보시스템에 보안위협이 존재하는지, 어떤 보안대책을 적용해야 할지 등을 세밀하게 파악할 필요가 있다.

이를 위해, 국가 망 보안체계는 다음 두 가지 보안원칙을 제시한다.

그림 1-12 정보서비스에 대한 모델 C/S/O 평가 및 보안원칙 적용



첫째, 「정보 생산·저장」 원칙이다. 기본적으로 정보시스템은 자신의 보안등급과 동일하거나 낮은 보안등급의 업무정보를 생산·저장할 수 있다. 그렇지 않은 경우, 보안대책이 필요하다. (‘✚’ 표시)

둘째, 「정보 이동」 원칙이다. 기본적으로 업무정보는 자신의 보안등급과 동일하거나 높은 보안등급의 정보시스템으로 이동할 수 있다. 그렇지 않은 경우, 보안대책이 필요하다. (‘✚’ 표시)

두 가지 보안원칙을 적용하면 위협의 유형과 보안대책 적용대상을 파악할 수 있고, 적절한 보안통제 항목을 선정하는 데 도움이 된다.

4. 보안통제 항목 선정

보안통제는 정보서비스 환경에서 식별된 위협에 대응하기 위한 보안대책을 의미하며, 국가 망 보안체계는 관리적·기술적 보안통제 항목으로 구성된다.

각 보안통제 항목은 국가·공공기관의 주요 정보서비스 모델에서 발생할 수 있는 위협을 예방·차단·탐지·대응·완화·복구 등의 보안대책을 구현할 수 있도록 설계되었다.

보안통제 항목 해설서(부록1)에 수록된 보안통제 항목은 ①권한, ②인증, ③분리 및 격리, ④통제, ⑤데이터, ⑥정보자산 등 6종의 대항목으로 구분되며, 세부 중항목 및 소항목으로 구성된다.

각 보안통제 항목은 실제 구현이 가능한 기술적 예시를 포함하여 각급기관의 정보보안 실무자가 특정 보안통제 항목의 구현을 위해서 필요한 기술개발 또는 도입이 필요한 제품군 등을 판단할 수 있다.

각 보안통제 항목은 고유한 식별자를 가지며, C/S/O 등급에 따른 우선 검토사항을 설정하고 있어 특정 보안등급을 가지는 업무정보·정보시스템에 대한 보안통제 항목 선택 시에 활용할 수 있다.

그림 1-13 **보안통제 항목 예시(부록1)**

국내 보안정책 반영
- 국가정보보안기본지침
- 각종 보안가이드라인 등

대항목	중항목	N2SF ID	소항목	보안통제 설명	N2SF 우선검토사항		
					C 기밀	S 민감	O 공개
권한	최소 권한 Least Privilege (LP)	N2SF-LP-1	정보시스템 접근 권한 정의	업무정보(데이터)를 식별하고, 업무정보를 저장하고 있는 정보시스템 접근 권한을 정의한다.	●	●	
		N2SF-LP-2	보안통제 권한 제한	보안통제 권한은 정보보안담당관(자) 또는 이에 준하는 관리권한을 부여받은 인원에게만 부여한다.	●	●	●
		N2SF-LP-3	보안통제 계정 노출 방지	보안통제 목적으로 사용되는 계정이 다른 기능에 사용되지 않도록 하고, 불필요한 사용을 제한하여 계정의 노출을 방지한다.	●	●	●
		N2SF-LP-4	관리자 권한 제한	정보시스템 접근에 필요한 최소한의 관리자 및 운영자 등에게만 관리자 권한을 부여한다.	●	●	
…							
통제	원격접속	N2SF-RA-1	원격접속 모니터링 및 통제	원격접속을 모니터링하고 통제한다.	●	●	
		N2SF-RA-2	원격접속 세션 암호화	원격접속 세션의 기밀성과 무결성을 보호하기 위해 통신 구간 암호화를 적용한다.	●	●	●

보안통제 분류 | 보안통제 항목 | C/S/O 등급별 우선검토사항

표 1-1 보안통제 항목의 구조 [예: 원격접속(Remote Access, RA)]

<table>
<tr><td rowspan="2">정의</td><td rowspan="2">원격접속환경에서의 기밀성과 무결성 강화를 위한 접속 통제 및 통신구간 암호화, 관리자·사용자의 접속 위치 및 권한 사용에 제한, 무단 정보 유출 방지 및 일정 시간 이후 세션 자동 종료와 같은 안전한 원격접속을 위한 통제항목이다.</td><td>구현 방법 예시</td><td>▸ 원격접속 모니터링 및 통제
– 원격 연결 세션은 SIEM을 통해 모든 접속 로그와 활동 이력을 실시간으로 수집하고 분석한다.
…
▸ 통신 구간 암호화 및 무결성 보장
– 원격접속은 TLS 1.2 이상 암호화 프로토콜을 적용한 SSH, HTTPS, VPN 등으로 구성하며, 강제 암호화 정책을 시스템 레벨에서 설정한다.
…
<table>
<tr><th>항목</th><th>적용 기술 또는 방식</th></tr>
<tr><td>접속 모니터링 및 감사</td><td>SEM, 접속 로그 수집, 사용자 위치/시간/행위 기반 탐지</td></tr>
<tr><td>통신 구간 암호화</td><td>TLS, SSH, HTTPS, VPN, mTLS, DH/ECDHE, 세션 무결성 검증</td></tr>
<tr><td>위치 기반 통제</td><td>GeoIP 기반 접근 제한, NAC 위치 정책, VPN 접근 제어</td></tr>
<tr><td>권한 제어 및 명령 제한</td><td>sudo 제한, 명령 화이트리스트, PAM, 관리자 계정 통제</td></tr>
<tr><td>정보 유출 방지</td><td>DLP, 클립보드 제한, 파일 전송 제어, FTP/SCP 무결정 검증</td></tr>
<tr><td>세션 자동 종료 및 비활성화</td><td>타임아웃 정책, MFA 재인증, 세션 자동 종료, 계정 자동 비활성화</td></tr>
<tr><td>명령 신뢰성 검증</td><td>명령 실행 전 MFA, OTP, 사전 등록 명령어 검증 시스템 적용</td></tr>
</table>
</td></tr>
<tr><td>보안 통제 항목 (소항목)</td><td>
<table>
<tr><th>N2SF ID</th><th colspan="2">보안통제 항목 설명</th></tr>
<tr><td rowspan="2">N2SF-RA-1</td><td>C S</td><td>원격접속 모니터링 및 통제</td></tr>
<tr><td colspan="2">원격접속을 모니터링하고 통제한다</td></tr>
<tr><td rowspan="2">N2SF-RA-2</td><td>C S O</td><td>원격접속 세션 암호화</td></tr>
<tr><td colspan="2">원격접속 세션의 기밀성과 무결성을 보호하기 위해 통신구간 암호화를 적용한다.</td></tr>
<tr><td rowspan="2">N2SF-RA-3</td><td>C S</td><td>원격접속위치통제</td></tr>
<tr><td colspan="2">보안관리 및 통제가 가능한 물리적 공간(위치) 또는 기술적 대책을 적용하여 원격접속을 허용한다.</td></tr>
<tr><td rowspan="2">N2SF-RA-4</td><td>C S</td><td>관리자 권한 통제</td></tr>
<tr><td colspan="2">원격접속을 통한 관리자 권한은 제한된 조건에서만 허용해야 하며, 관리자 권한으로 실행한 명령어 이력 등은 유지한다.</td></tr>
<tr><td rowspan="2">N2SF-RA-5</td><td>C S O</td><td>원격접속 정보 유출 방지</td></tr>
<tr><td colspan="2">원격접속에 관한 정보를 무단으로 사용하거나 외부로 유출되는 것을 방지한다.</td></tr>
<tr><td rowspan="2">N2SF-RA-6</td><td>C S O</td><td>원격접속 자동 종료 및 비활성화</td></tr>
<tr><td colspan="2">일정기간 경과 등 조건에 따라 원격접속을 자동 종료하거나, 원격접속 목적이 달성된 경우 비활성화한다.</td></tr>
<tr><td rowspan="2">N2SF-RA-7</td><td>C S</td><td>원격 명령 신뢰성 검증</td></tr>
<tr><td colspan="2">명령을 수행하기 전에 적절한 인증 체계(암호화된 인증서, 보안 토큰, 또는 사용자 인증)를 적용하여 명령의 무결성과 출처를 검증한다.</td></tr>
<tr><td rowspan="2">N2SF-RA-M1</td><td>C S</td><td>원격접속 정책 수립 및 예외 관리</td></tr>
<tr><td colspan="2">원격접속 허용 대상, 시간, 인증수단 등에 대한 정책을 수립하고 예외 시 승인 절차를 마련한다.</td></tr>
<tr><td rowspan="2">N2SF-RA-M2</td><td>C S</td><td>원격접속 로그 보존 및 감사</td></tr>
<tr><td colspan="2">원격접속 활동 기록을 수집하여 정기 감사가 가능하도록 보존한다.</td></tr>
<tr><td rowspan="2">N2SF-RA-M3</td><td>C S</td><td>원격접속 보안 점검 주기 운영</td></tr>
<tr><td colspan="2">원격접속 정책 이행 여부와 취약 구성 점검을 주기적으로 수행한다.</td></tr>
</table>
</td></tr>
</table>

제4절

고려사항

1. 보안업무 절차와 인식의 틀에 N2SF정착 필요

국가 망 보안체계는 국가·공공기관이 일관된 방법으로 정보서비스의 위협을 식별하고 위험 수준을 평가하여, 적절한 보안대책을 수립·구현·운영하며 보안수준을 유지할 수 있도록 하는 일련의 지침과 원칙이다.

따라서, 국가 망 보안체계를 통해 국가·공공기관의 보안 수준을 실질적으로 향상시키려면, 각 단계별 활동을 기관의 실제 정보보안 업무 절차에 반영하여 보안 인식의 기본 틀로 확립하는 노력이 필요하다.

2. 기관 특성과 환경을 반영한 맞춤형 보안대책 수립

보안대책 수립 시에는 기관별·정보서비스별 특성과 사이버공격의 양상 등을 반영할 수 있으며, 보안통제 항목의 선택 및 구현 시 조직의 기술적 상황(목표 보안수준, 호환성 등)뿐만 아니라 비기술적 여건(관련 규정, 예산, 인력 등)도 함께 반영하는 것이 바람직하다.

3. 정보서비스 모델 해설서(부록2)의 활용

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 구축할 수 있다. 정보서비스 모델은 지속적으로 개발·제공될 예정이다.

해설서에 수록된 정보서비스 모델과 동일한 정보서비스를 구축하는 경우 해설서를 토대로 N2SF 최종 산출물(자체 보안대책 등)을 작성하여 보안성 검토 시에 활용할 수 있다.

만약, 해설서에 수록된 모델의 구조에서 일부를 변경하거나 추가하는 경우 영향받는 부분에 대한 위협식별, 보안대책 수립 등의 단계를 고려하여 수행해야 한다.

4. 기관 업무·기능 범위 설정과 BRM 연계

각급기관은 정보화사업에 포함된 정보서비스 범위 내에서 관련 업무·기능을 분석한다. 기관 업무·기능 분석을 위한 BRM 연계는 업무 중요도·우선순위·보안등급 판단 시에 기관이 자율적으로 수행할 수 있다.

5. 추가 보안통제 항목 정의 및 적용

본 가이드라인의 부록1(보안통제 항목 해설서)은 일반적인 정보서비스 모델에서 활용되는 보안대책을 제공한다.

하지만 정보서비스의 구조나 식별된 위협의 특성 등에 따라 각급기관이 자체적으로 추가 보안통제 항목을 정의하고 구현할 수 있다.

6. N2SF 적용 시 관련 지침·가이드라인 고려

국가 망 보안체계(N2SF) 보안 가이드라인은 각급기관이 정보서비스를 설계·구축·운영할 때 필요한 자체 보안대책을 수립하기 위해 공통적으로 요구되는 최소한의 절차와 방법을 제공한다.

따라서 국가 망 보안체계를 통해 자체 보안대책 수립 시에는 해당 정보서비스와 관련된 지침·가이드라인 등을 충분히 고려해야 한다.

예를 들어, 클라우드 기반 협업 도구를 활용할 경우 「국가 클라우드 컴퓨팅 보안 가이드라인」, 생성형 AI를 활용하는 경우 「챗GPT 등 생성형 AI 활용 보안 가이드라인」 등 관련 보안 가이드라인에서 제시하는 요구사항을 충족하도록 국가 망 보안체계 5단계 절차를 수행해야 한다.



국가 망 보안체계
보안 가이드라인

제2장

국가 망 보안체계(N2SF) 적용 절차

제1절 준비(Prepare)

제2절 C/S/O 등급분류(Categorize)

제3절 위협식별(Identify)

제4절 보안대책 수립(Select)

제5절 적절성 평가·조정(Assess)

국가 망 보안체계는 정보화사업 추진 시 정보서비스에 대한 자체 보안대책 수립에 활용하며 ❶준비(Prepare), ❷C/S/O 등급분류(Categorize), ❸위협식별(Identify), ❹보안대책 수립(Select), ❺적절성 평가·조정(Assess) 등 5단계 절차로 구성된다.

표 2-1 국가 망 보안체계 단계별 주요활동(요약)

단계	주요활동(요약)
❶ 준비 (Prepare)	▸ [활동-1-1] N2SF 적용계획 수립 ▸ [활동-1-2] 기관 업무·기능 분석 ▸ [활동-1-3] 업무정보 식별 ▸ [활동-1-4] 정보시스템 식별 ▸ [활동-1-5] 정보서비스 식별
❷ C/S/O 등급분류 (Categorize)	▸ [활동-2-1] 업무정보 C/S/O 분류 ▸ [활동-2-2] 정보시스템 C/S/O 분류
❸ 위협식별 (Identify)	▸ [활동-3-1] 모델링 및 C/S/O 평가 ▸ [활동-3-2] 보안원칙 적용 ▸ [활동-3-3] 보안위협 식별
❹ 보안대책 수립 (Select)	▸ [활동-4-1] 보안 요구사항 도출 ▸ [활동-4-2] 보안통제 선택
❺ 적절성 평가·조정 (Assess)	▸ [활동-5-1] 적절성 평가 ▸ [활동-5-2] 적절성 평가결과 협의·조정 ▸ [활동-5-3] 적절성 평가결과 확인

국가 망 보안체계의 원활한 적용 및 운영을 위해서 각급기관은 각 단계에서 수행해야 할 주요활동을 명확히 숙지해야 한다. 본 가이드라인에서 최종 산출물(자체 보안대책)의 서식을 제공하므로 이를 보안성 검토 시 활용할 수 있다.

제1절 준비(Prepare)

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

표 2-2 준비(Prepare) 단계 주요활동별 수행내용

단계	주요활동	수행내용
❶ 준비 (Prepare)	[활동-1-1] N2SF 적용계획 수립	▸ 단계별 책임자 지정 및 역할·권한 정의 – 적절성 평가·조정 단계 책임자는 정보보안담당관
		▸ 단계별 요구사항 정의, 수행일정 수립 등
	[활동-1-2] 기관 업무·기능 분석	▸ 본 정보화사업 범위에 해당하는 정부기능분류체계, 지방기능분류체계, 지방교육기능분류체계 등에 따른 기관업무·기능 분석을 통해 BRM 수립 – 정보서비스 업무·기능 식별 (레벨5 이하 권고)
	[활동-1-3] 업무정보 식별	▸ 본 정보화사업 범위에 해당하는 정보서비스의 업무·기능 수행 시 생산, 저장, 처리, 이동, 보관, 폐기되는 업무정보 식별 – 기관 업무·기능에 대한 업무정보 관계 파악
	[활동-1-4] 정보시스템 식별	▸ 업무정보의 생산, 저장, 처리, 이동, 보관, 폐기에 관여하는 정보시스템 식별 – 정보시스템의 물리적·논리적 구성, 업무정보 관련성 등 파악
	[활동-1-5] 정보서비스 식별	▸ 네트워크, 정보시스템, 업무정보 등 정보서비스 구성 및 구조 분석
		▸ 정보서비스 이용 및 용도에 따른 다양한 사용 시나리오 정의 – 1개 이상의 사용 시나리오 가능
		▸ 정보서비스의 보안목표(기초 보안 요구사항) 설정 – 정보서비스 사용 시나리오 고려 – 관련 지침, 가이드라인 등 참고

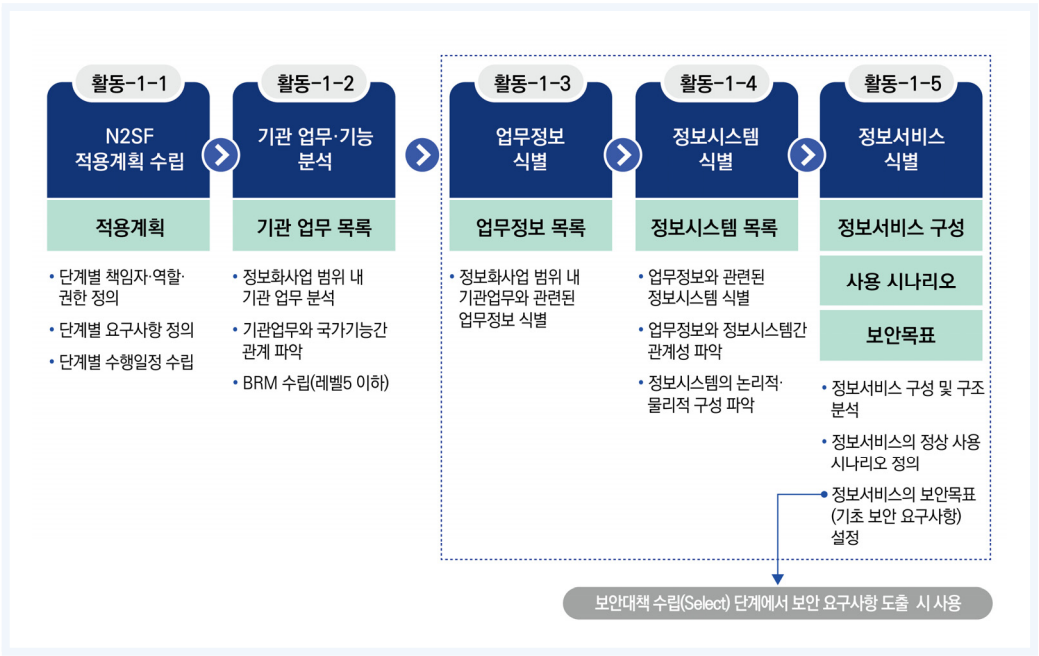
준비 단계에서 가장 중요한 활동은 해당 정보서비스와 관련된 기관의 업무·기능을 분석하고 각 업무와 관련된 업무정보와, 업무정보를 취급하는 정보시스템을 식별한 후, 정보서비스의 논리적·

물리적 구성 및 구조를 파악하는 것이다.

그리고, 정보서비스의 목적과 용도를 감안하여 사용 시나리오를 정의한다.

또한, 정보서비스에 대한 기초 보안 요구사항인 보안목표를 설정한다. 보안목표 설정에는 정보서비스의 시나리오 및 기관에 적용되는 정보보안 관련 지침, 가이드라인 등을 참고할 수 있다.

그림 2-1 준비(Prepare) 단계 주요활동 흐름도



1. N2SF 적용계획 수립 [활동-1-1]

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.

필요시 각 단계의 활동별 세부 책임자를 지정할 수 있다. 또한, '기관 업무·기능 분석', '업무정보 식별', '정보시스템 식별' 등 정보보안 담당자가 단독으로 수행하기 어려운 활동의 경우 인사·조직 담당자, 정보화 담당자 등을 공동 책임자로 지정한다.

표 2-3 N2SF 적용계획 수립[활동-1-1]의 세부활동

수행내용	설명	비고
단계별 책임자 지정	단계별 책임자 지정	필요시 단계 내 활동별 세부 책임자 별도 지정 가능
		객관성 및 책임성 확보를 위해 적절성 평가·조정 단계의 책임자는 정보보안담당관으로 지정
역할 및 책임 정의	단계별 책임자의 역할, 권한 등 정의	정보보안 담당자와 정보화 담당자 등과 협업하는 경우 역할 분담
		적절성 평가·조정 결과에 따른 일부 활동 재수행 고려
단계별 요구사항 정의	단계별 요구사항 정의	기관 업무기능 분석, 업무정보 식별, 정보시스템, 정보서비스 식별 등 정보보안 담당자가 단독으로 수행이 어려운 활동은 정보화 담당자 등과 협업
단계별 수행일정 수립	단계별 수행일정 수립	보안성 검토 일정 등을 감안하여 N2SF 각 단계별 수행일정 수립

2. 기관 업무·기능 분석 [활동-1-2]

기관 업무·기능 분석은 기관의 전체 업무·기능 중에서 정보화사업의 범위 내의 업무·기능을 대상으로 분석한다.

국가·공공기관의 업무·기능을 분석하기 위해서는 ①정부기능분류체계, 지방기능분류체계, 지방교육기능분류체계 등(이하 '공공 BRM')을 사용하거나 ②기관의 자체적인 기능분류체계(이하 '자체 BRM')를 사용할 수 있다.

BRM의 중기능(4레벨)은 중앙행정기관의 '과' 수준의 기능을 뜻하며 하나의 '과' 내에 서로 다른 보안등급의 업무를 수행할 수 있으므로, 공개 가능한 업무가 비공개 업무로 판단되거나 비공개 업무가 공개 업무로 판단될 우려가 있다. 따라서, 최소 소기능(5레벨) 또는 단위과제(6레벨) 수준까지 세분화하여 국가의 기능과 기관의 업무를 분석할 것을 권고한다.

국가 BRM은 중앙행정기관의 정책분야(1레벨)부터 소기능(5레벨) 수준까지 포함돼 있으므로 하위기관은 상위기관의 관련 기능을 '상위과제ID'로 설정한 단위과제(6레벨)를 자체 BRM으로 구성하여 연계할 수 있다.

물론, 기관의 특정 업무·기능의 계층 구조가 국가 BRM에서 대기능(3레벨)까지만 식별된다면, 기관은 자체 BRM으로 중기능(4레벨) 이하의 업무기능을 정의하고 공식 BRM의 대기능(3레벨)을 중기능(4레벨)의 '상위과제ID'로 설정하여 BRM 체계를 완성할 수 있다.

그림 2-2 정부기능분류체계 (출처: 국가기록원)

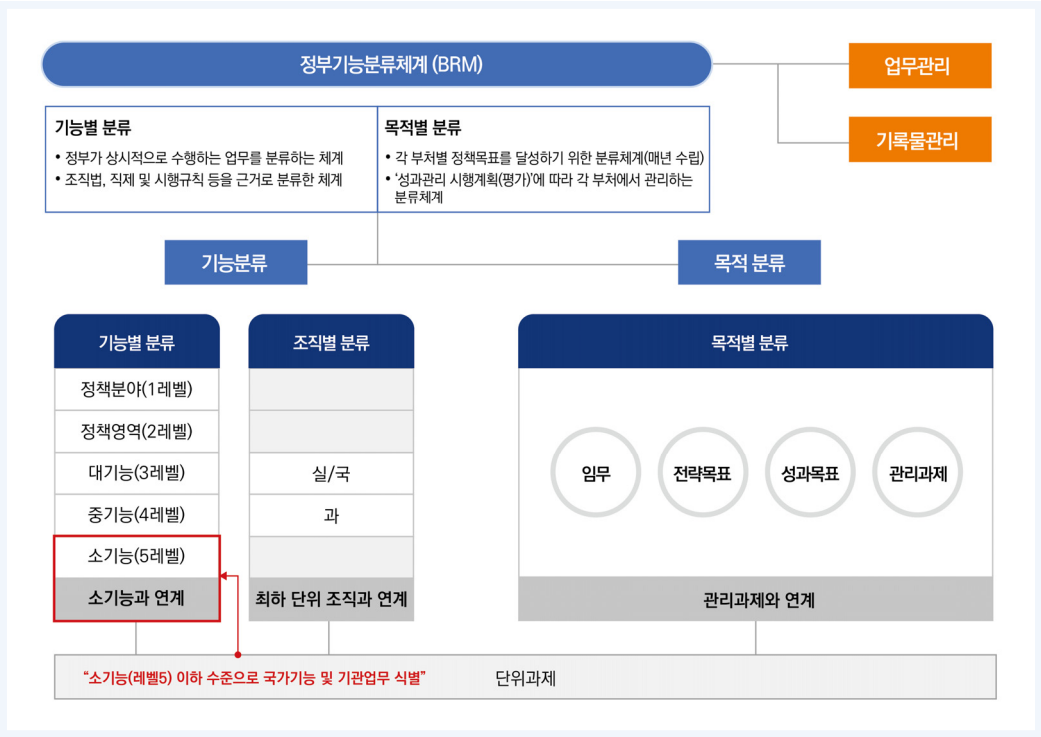
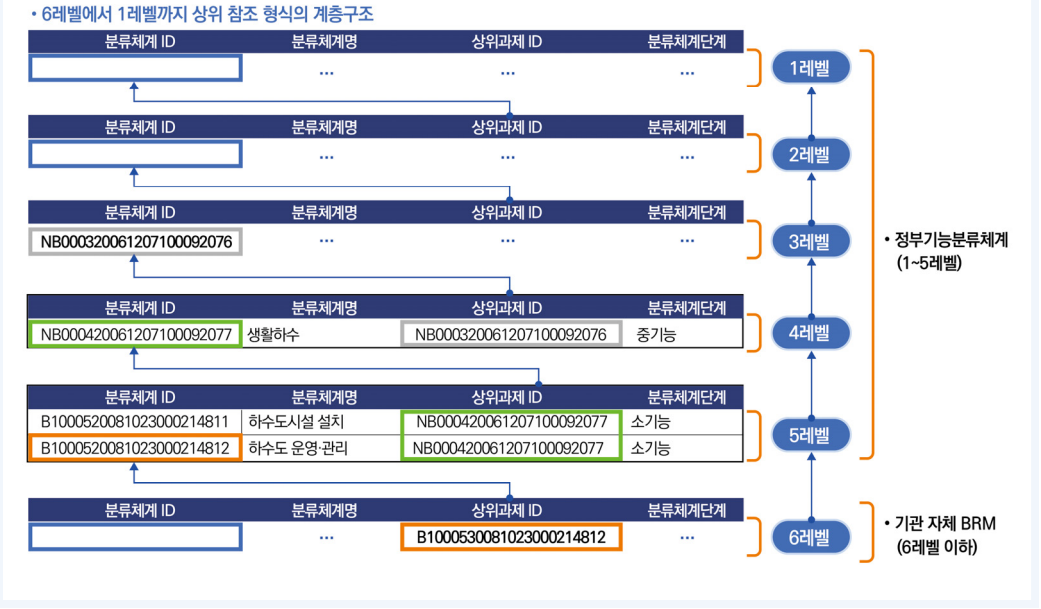


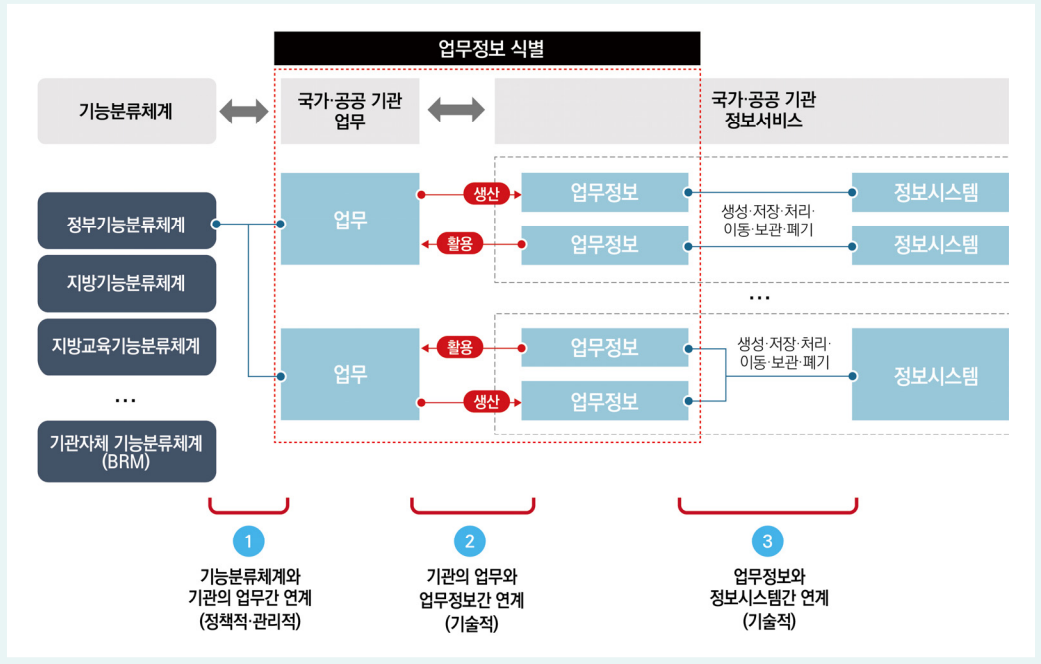
그림 2-3 정부기능분류체계와 기관 자체 BRM 연계 예시



3. 업무정보 식별 [활동-1-3]

업무정보는 정보서비스를 통해서 수행되는 기관의 업무에 필요한 정보 또는 업무의 결과로 생산되는 공공데이터를 의미한다.

그림 2-4 업무정보 식별 개념도



다음 표는 특정 정보서비스에 대해서 식별된 업무정보를 목록화한 예시이다. 업무정보의 명칭, 업무정보에 관한 설명, 데이터형식 등을 식별할 수 있다.

표 2-4 업무정보 식별 예시

기관 업무 (BRM)	업무정보	형식
OO기술 연구개발	인터넷 수집자료	문서, 이미지, 동영상 등
	인터넷 수집자료 취합문서	문서(hwp, ppt 등)
	연구 보고서	문서(hwp)
	SW 설계서 및 소스코드	문서(hwp), Python

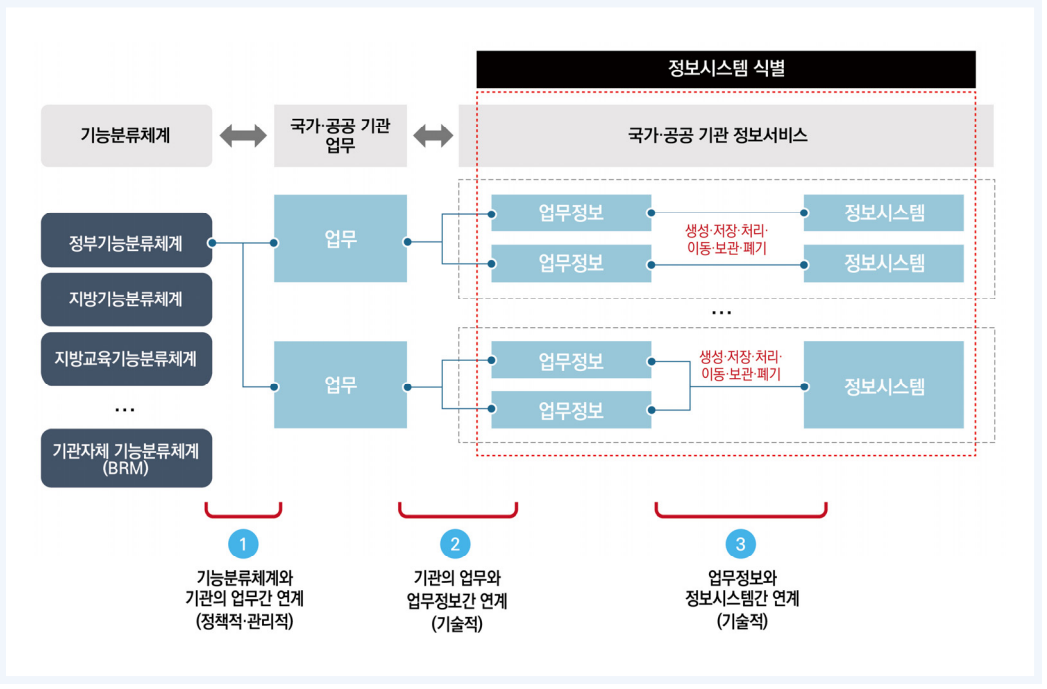
4. 정보시스템 식별 [활동-1-4]

정보시스템 식별 단계에서는 ①정보시스템과 업무정보의 관계를 파악하고, ②정보시스템의 논리적·물리적 구성 및 특징을 분석한다.

①정보시스템은 업무정보의 생성·저장·처리·이동·보관·폐기 등에 관여하는 시스템을 말한다. 각 업무정보의 생명주기를 파악하는 과정에서 해당 업무정보와 관련된 정보시스템을 식별할 수 있다. 또한, 정보서비스의 특성에 따라 외부 정보서비스(예: 간편인증, 생성형 AI, SaaS 등)와 연동되는 경우 함께 식별한다.

②정보시스템의 구성 및 특징을 분석하는 방법과 수준은 정보화사업의 성격에 따라 결정된다. 최초 구축 형태의 정보화사업의 경우, 정보시스템이 설계 단계에 있어 구체적인 정보를 식별하기 어렵다. 반면, 기존 정보서비스에 일부 기능을 추가하거나 개선하는 정보화사업의 경우에는 정보시스템의 구체적인 정보(예: HW사양, 모델명, SW사양 등)를 파악하여 이후 위협식별 단계에서 활용할 수 있다.

그림 2-5 정보시스템 식별 개념도



5. 정보서비스 식별 [활동-1-5]

정보서비스 식별 활동에서는 ①네트워크, 정보시스템, 업무정보 등 정보서비스의 구성 및 구조를 분석하고, ②정보서비스의 목적과 용도에 따른 사용 시나리오를 정의하며, ③정보서비스의 보안목표(기초적인 보안 요구사항)를 설정한다.

①정보서비스의 구성 및 구조 분석 시에는 기관 내부뿐만 아니라 기관 외부 정보서비스와의 연동에 대해서도 면밀하게 분석한다.

②정보서비스 사용 시나리오는 정상적인 정보서비스의 기능을 사용하는 시나리오를 뜻하며, 해당 사용 시나리오와 관련된 정보시스템을 함께 식별한다.

사용 시나리오 정의는 이후 위협식별 단계와 매우 밀접한 관계를 가진다. 사용 시나리오가 개괄적으로 정의되면 식별 가능한 위협을 간과할 위험이 있고, 세밀하게 정의되면 위협식별 과정에 지나치게 많은 시간과 노력이 소요된다. 따라서, 정보서비스 구성상 보안등급 간 경계, 보안통제 적용지점 등을 파악할 수 있는 수준으로 사용 시나리오를 정의한다.

표 2-5 정보서비스 사용 시나리오 정의 예시

사용 시나리오	관련 정보시스템	비고
연구단말에서 인터넷의 연구자료를 수집	연구단말, 인터넷	
연구단말에서 연구보고서를 작성하고 연구시스템으로 업로드	연구단말, 연구시스템	
…		

③기관에 적용받는 관련 지침·가이드라인, 정보서비스의 특성 등에 따른 기초적인 보안 요구사항으로서 보안목표를 설정할 수 있다. 보안목표는 이후 보안대책 수립 단계에 반영된다.

표 2-6 정보서비스 보안목표 설정 예시

보안목표	근거
업무영역과 별도로 연구망 구성 (연구망 침해 시 피해 전이 방지)	OO부 정보보안기본지침
연구목적에 필요한 인터넷 서비스만 접속	자체
인터넷과 연구시스템 동시연결 차단	자체

제2절

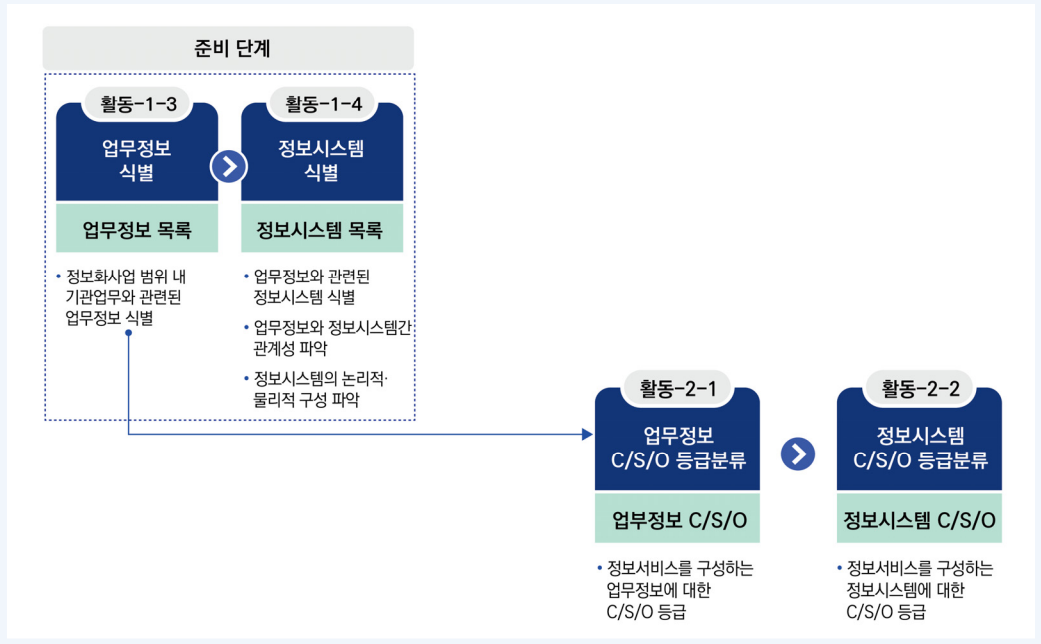
C/S/O 등급분류(Categorize)

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

표 2-7 C/S/O 등급분류 단계 주요활동별 수행내용

단계	주요활동	수행내용
❷ C/S/O 등급분류 (Categorize)	[활동-2-1] 업무정보 C/S/O 등급분류	▸ 업무정보의 C/S/O 등급분류 – 준비 단계에서 식별된 업무정보에 대한 C/S/O 등급분류
	[활동-2-2] 정보시스템 C/S/O 등급분류	▸ 업무정보의 생산·저장·처리·이동·보관·폐기 등에 관여하는 정보시스템의 C/S/O 등급분류

그림 2-6 C/S/O 등급분류(Categorize) 단계 주요활동 흐름도



1. 업무정보 C/S/O 등급분류 [활동-2-1]

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. 아래 표는 「정보공개법」, 「공공데이터법」 등 관련 법령에 근거하여 C/S/O 등급분류 기준을 마련한 것이다.

표 2-8 업무정보에 대한 C/S/O 등급분류 기준

등급	C/S/O 등급분류 기준	비고
기밀 (C)	▸ 제1호: 법률상 비밀·비공개로 규정 ▸ 제2호: 안보·국방·통일·외교 관련 공개 시 국익 저해 ▸ 제3호: 공개 시 국민 생명·신체·재산보호에 현저한 지장초래 ▸ 제4호: 진행 중 재판 및 범죄예방·수사·공소·형집행·교정 관련 정보로, 공개 시 현저한 직무수행 곤란 및 피고인 재판권 침해	정보 공개법 공공 데이터법
민감 (S)	▸ 제5호: 감사·감독·검사·시험·입찰계약·기술개발·인사관리 및 의사결정·내부검토 관련 정보로, 공개 시 공정한 업무수행, 연구개발 등에 현저한 지장 ▸ 제6호: 성명·주민번호 등 개인정보로, 공개 시 사생활 침해 ▸ 제7호: 법인·단체·개인의 경영상·영업상 비밀로, 공개 시 이익 침해 ▸ 제8호: 공개 시 부동산투기, 매점매석으로 특정인에게 이익·불이익	
	▸ 기 타: 로그 및 임시백업 등	
공개 (O)	▸ 기밀(C)·민감(S) 정보 이외의 정보	
	▸ 관련 법령 등에서 규정하는 요건을 충족한 비공개 정보 또는 기간의 경과 등으로 비공개 필요성이 소멸된 정보	

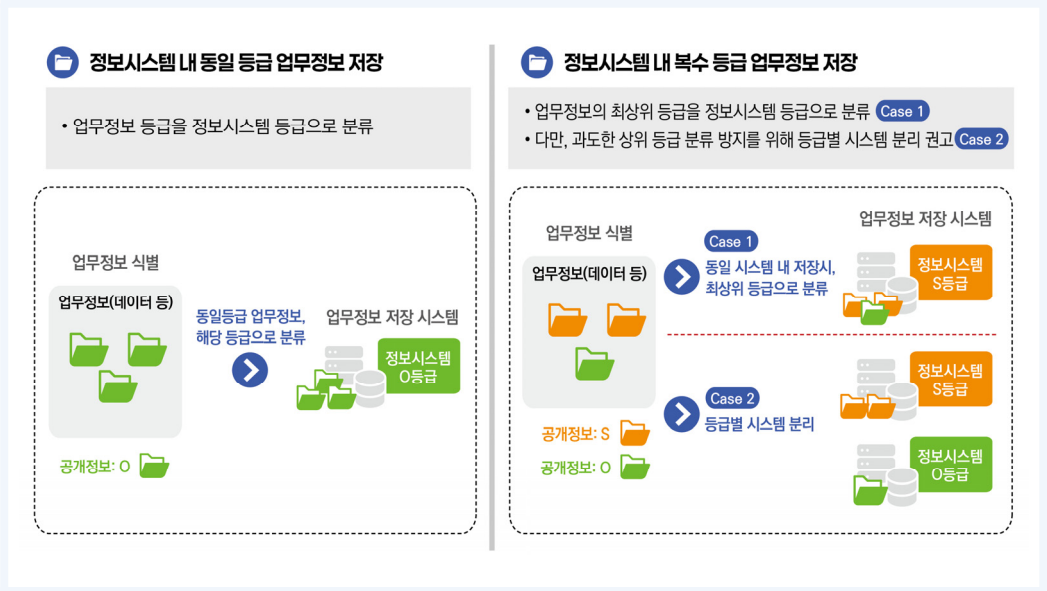
2. 정보시스템 C/S/O 등급분류 [활동-2-2]

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

다음 그림은 동일 등급의 업무정보로 구성된 정보시스템(좌)과 복수 등급의 업무정보로 구성된 정보시스템(우)에 대한 각각의 C/S/O 등급분류 방법을 설명하고 있다.

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

그림 2-7 정보시스템의 C/S/O 등급분류 기준 (좌: 동일 등급의 경우, 우: 복수 등급의 경우)



복수 등급의 경우 두 가지 방법(Case 1, Case 2)을 적용할 수 있는데, 이에 대한 장단점 및 주의사항을 정리하면 다음 표와 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 보안 측면에서 가장 명확한 분류 방법이나 정보시스템 구성의 변화에 따른 시스템 구축, SW 개발, 유지보수 등의 추가 비용이 소요될 수 있다.

따라서, 동일 등급의 업무정보별로 정보시스템을 분리하여 구축하는 것이 원칙상 가장 명확하고 공공데이터의 활용 측면에서도 바람직하나 분리 구축에 따른 비용 소요 등 각급기관의 현실적인 상황을 충분히 고려해야 한다.

표 2-9 정보시스템에 대한 C/S/O 등급분류 예시 및 주의사항

구성	업무정보 보안등급	조건	정보시스템 보안등급	
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	
		Case 2 시스템 분리	S	O
	C + S	Case 1 상위등급으로 분류	C	
		Case 2 시스템 분리	C	S
	C + O	Case 1 상위등급으로 분류	C	
		Case 2 시스템 분리	C	O

제3절

위협식별(Identify)

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

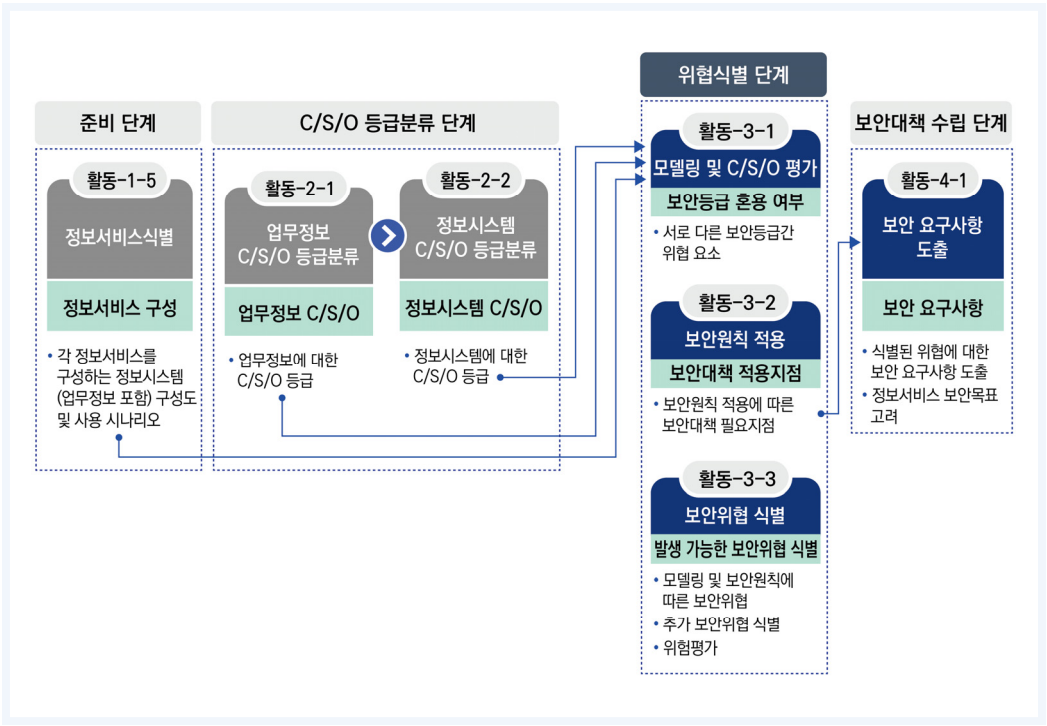
표 2-10 위협식별(Identify) 단계 주요활동별 수행내용

단계	주요활동	수행내용
❸ 위협식별 (Identify)	[활동-3-1] 모델링 및 C/S/O 평가	▸ 정보서비스 사용 시나리오에 대한 「위치-주체-객체」 모델링 및 C/S/O 평가를 통해 보안등급 차이에 따른 보안대책 필요 여부 판단
	[활동-3-2] 보안원칙 적용	▸ 정보서비스 사용 시나리오별 「위치-주체-객체」 모델을 기반으로 「정보 생산·저장」 및 「정보 이동」의 보안원칙 적용으로 보안대책 필요 지점 파악
	[활동-3-3] 보안위협 식별	▸ 「위치-주체-객체」 모델링 및 C/S/O 평가, 보안원칙 적용 결과를 기반으로 서로 다른 보안등급 간 발생 가능한 보안위협 식별

정보서비스 위협 모델링을 위해서는 준비 단계에서 식별한 정보서비스 구성 정보와 C/S/O 등급분류 단계에서 결정된 업무정보·정보시스템·위치에 대한 C/S/O 등급분류 결과가 필요하다.

정보서비스 위협 모델링을 수행하면 그 결과로 서로 다른 보안등급이 식별되어 보안대책 적용지점과 위협의 유형 등을 도출할 수 있다.

그림 2-8 위협식별(Identify) 단계의 주요활동 흐름도



위협을 식별하고 그 위험을 평가하며 적절한 보안대책을 수립하는 과정에서, 모든 국가·공공기관에 적합한 기술적 수준의 방법론을 제시하는 것은 매우 어렵다.

이는 교육, 전력, 과학, 치안, 복지 등 공공부문별 산업군과 그에 따른 기관의 업무와 기능이 상이하며, 기관별로 다루는 업무정보와 이를 저장·처리하는 정보시스템의 구성 형태, 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 위협식별 방법론으로 「위치-주체-객체」 모델링을 제시하며, 세부적인 보안원칙으로서 「정보 생산·저장」 원칙, 「정보 이동」 원칙을 제시한다.

부록2(정보서비스 모델 해설서)는 특정 정보서비스 모델에 대한 위협식별 및 필요한 보안통제 항목 등을 안내하고 있으므로 유사한 정보서비스 모델의 경우 위협식별 단계 및 보안대책 수립 단계에서 참고할 수 있다.

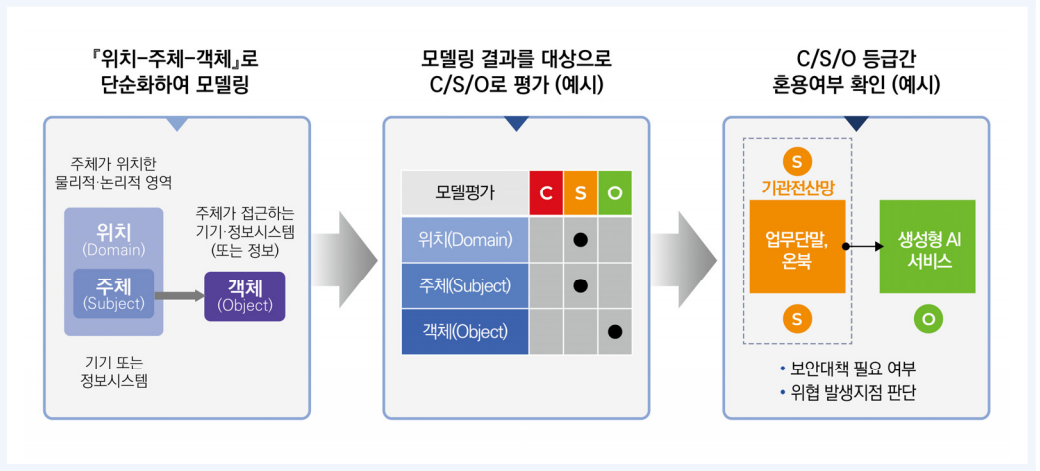
1. 모델링 및 C/S/O 평가 [활동-3-1]

정보서비스 구성, C/S/O 등급, 사용 시나리오 등을 토대로 「위치-주체-객체」 모델링 및 C/S/O 평가를 통해 보안등급 차이에 따른 보안대책 필요 여부를 판단한다.

「위치-주체-객체」 모델링을 위해서는 정보서비스를 활용하는 정보시스템(단말 등)을 주체로 식별하고, 정보서비스를 제공하는 정보시스템(서버 등)을 객체로 식별한다. 또한 주체의 물리적·논리적 위치도 식별한다.

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

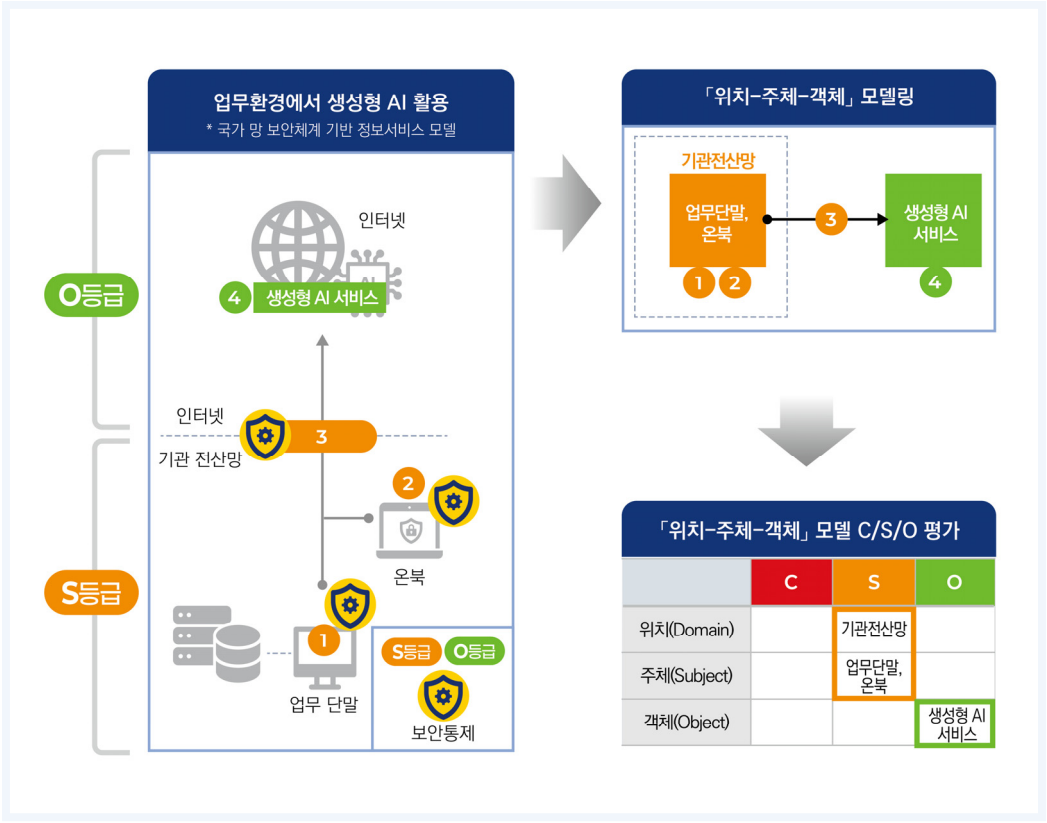
그림 2-9 「위치-주체-객체」 모델링 및 C/S/O 평가 개념도



만약 「위치-주체-객체」 모델 평가표에 보안등급 서로 다른 등급에 위치한다면, 해당 정보서비스 사용 시나리오는 정상적인 상태에서 C/S/O 등급 간 혼용이 발생하므로 보안대책이 필요하며, 위협의 양상과 구체적인 보안대책 적용지점을 파악하기 위해 두 가지(「정보 생산·저장」 및 「정보 이동」) 보안원칙을 적용해야 한다.

다음 그림은 정보서비스 모델 예시에 대한 「위치-주체-객체」 모델링과 C/S/O 평가 과정을 나타낸다. 본 위협식별 단계의 이해도를 높이기 위해서 '업무환경에서 생성형 AI 활용'을 예시로 활용한다.

그림 2-10 「위치-주체-객체」 모델링 및 C/S/O 평가 예시 (업무환경에서 생성형 AI 활용)



기관전산망에서 업무단말 및 온북을 이용해서 인터넷에 위치한 생성형 AI 서비스를 이용하는 사용 시나리오이며, 위치(기관전산망)와 주체(업무단말❶ 및 온북❷)는 모두 S등급이고 객체(생성형 AI 서비스❹)는 O등급에 해당한다.

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

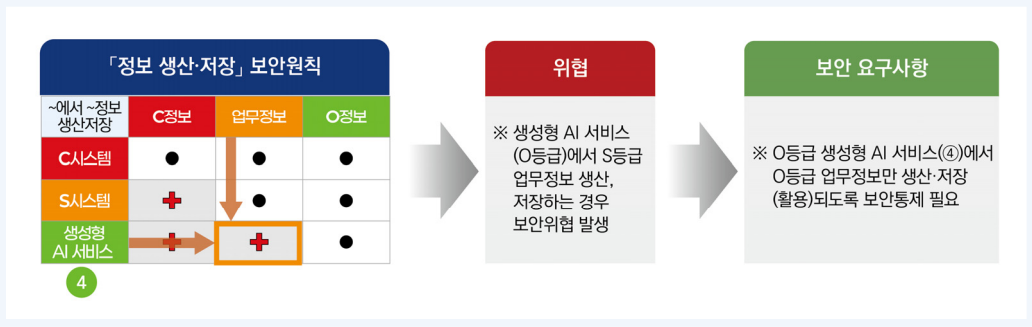
2. 보안원칙 적용 [활동-3-2]

보안원칙은 「정보 생산·저장」과 「정보 이동」으로 구성되며, 「위치-주체-객체」 모델링 및 C/S/O 평가와 연동해서 적용한다.

가. 「정보 생산·저장」 보안원칙

「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.

그림 2-11 「정보 생산·저장」 보안원칙 적용 예시 (업무환경에서 생성형 AI 활용)



위의 그림은 정보서비스 모델 예시에 대한 「정보 생산·저장」 보안원칙 적용 과정을 나타낸다.

생성형 AI 서비스(O등급)에서 S등급 업무정보가 생산·저장되는 위협을 발견할 수 있으며, 이를 해결하기 위해서는 생성형 AI 서비스④에서 O등급 업무정보만 취급하도록 하는 보안통제가 필요함을 알 수 있다.

나. 「정보 이동」 보안원칙

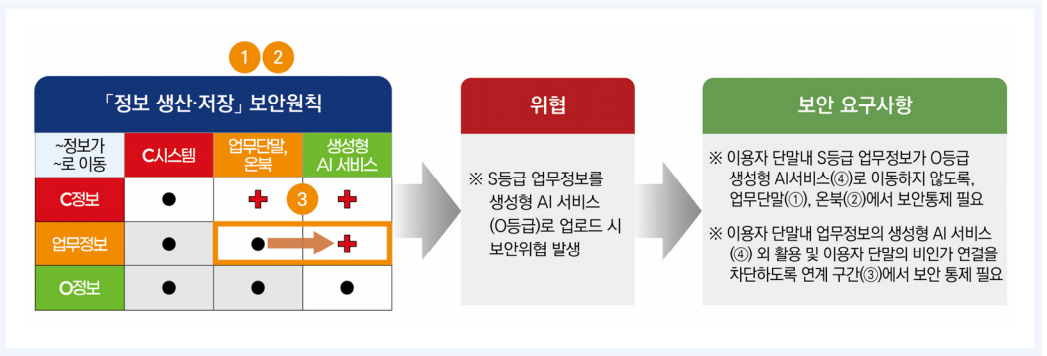
「정보 이동」 보안원칙은 업무정보가 각 정보시스템으로 이동할 때, 업무정보의 보안등급보다 낮은 등급의 정보시스템으로 이동이 발생하는 것을 위협으로 식별한다. 마찬가지로, 위협식별 영역에는

'✚' 표시가 있다.

다음 그림은 정보서비스 모델 예시에 대한 「정보 이동」 보안원칙 적용 과정을 나타낸다. 업무단말❶과 온북❷에서 생성형 AI 서비스❹로 S등급 업무정보를 업로드하여 처리·가공할 수 있으므로 위협으로 식별된다.

이를 해결하기 위해서는 업무단말❶과 온북❷에서 S등급 업무정보의 업로드를 차단하고 연계구간❸에서 이를 필터링하는 등의 보안통제가 필요함을 알 수 있다.

그림 2-12 「정보 이동」 보안원칙 적용 예시 (업무환경에서 생성형 AI 활용)



3. 보안위협 식별 [활동-3-3]

본 가이드라인이 제시하는 위협식별 방법론인 「위치-주체-객체」 모델링 및 C/S/O 평가, 보안원칙 적용 등을 통해서 서로 다른 보안등급 간 발생 가능한 보안위협(정보유출 유형)을 식별할 수 있다.

만약 취약점, 악성코드, DoS(서비스거부), 공급망 공격, 내부자 위협 등 다양한 보안위협을 충분히 고려하고자 한다면 위협 모델링 SW, 취약점 진단, 모의해킹, CTI(사이버위협인텔리전스) 등의 추가적인 위협식별 활동이 필요하다.

또한, 식별된 보안위협에 대해 발생 가능성, 파급력 등을 종합적으로 판단하는 위험평가 방법론을 적용하여 보안대책 수립·구현 시 우선순위 등에 반영하는 것을 고려할 수 있다.

제4절

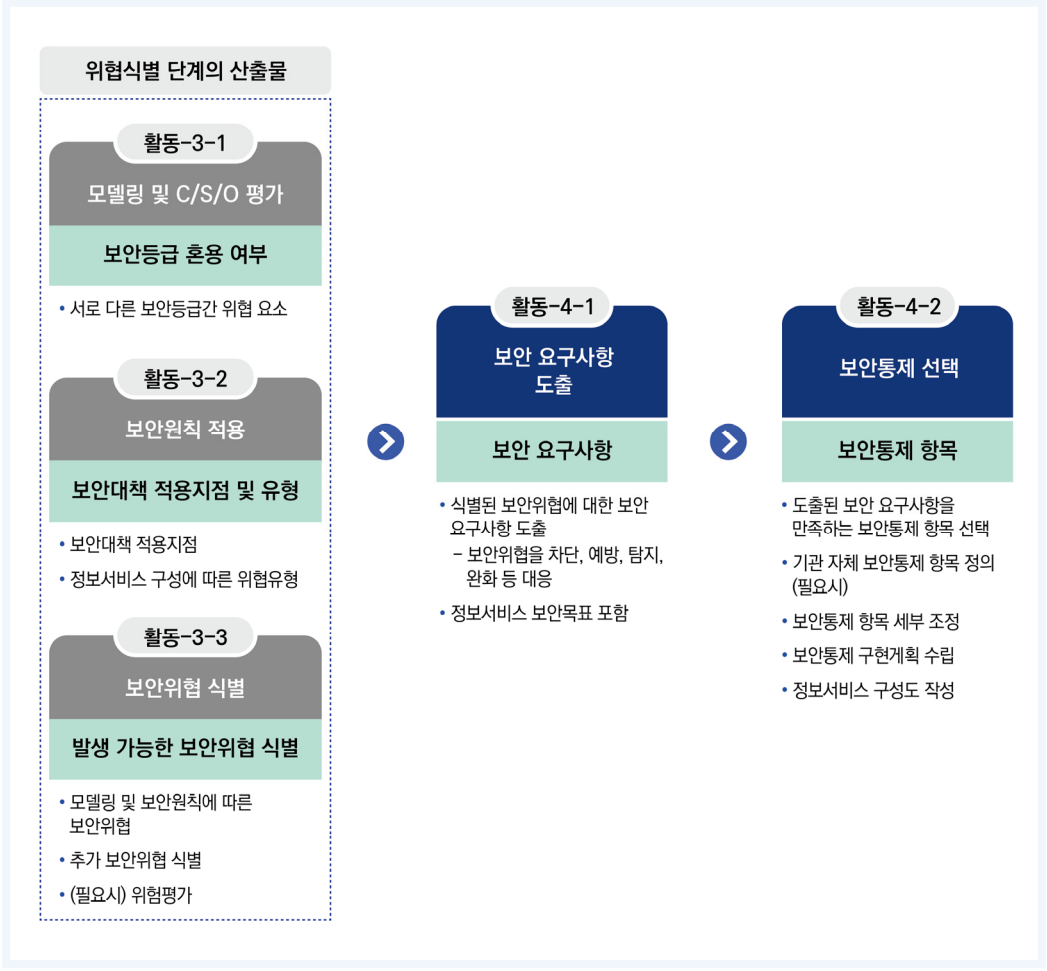
보안대책 수립(Select)

보안대책 수립 단계에서는 앞선 위협식별 단계에서 식별된 보안위협을 해소하기 위한 보안 요구사항을 도출하고, 보안 요구사항을 만족하는 관리적·기술적 수단으로서의 보안통제 항목을 선택한다. 그런 다음, 보안통제 구현계획을 수립한다.

표 2-11 보안대책 수립(Select) 단계 주요활동별 수행내용

단계	주요활동	수행내용
❹ 보안대책 수립 (Select)	[활동-4-1] 보안 요구사항 도출	‣ 식별된 보안위협에 대한 보안 요구사항 도출 – 기관의 특성, 업무정보·정보시스템·정보서비스 특성 등에 따라 다양하게 도출 가능 – 준비단계에서 설정한 정보서비스 보안목표를 보안 요구사항에 포함
	[활동-4-2] 보안통제 선택	‣ 도출된 보안 요구사항을 만족하는 관리적·기술적 수단으로서의 보안통제 항목 선택 – C/S/O 등급에 따른 우선 검토사항 고려 – N2SF 기본 보안통제 항목 외에 추가적인 보안통제 항목을 각급기관이 자체적으로 정의하여 사용 가능 – 정보서비스 보안목표, 업무정보·정보시스템·정보서비스 특성, 보안통제 특성 등에 따른 세부사항 조정 가능
		‣ 보안통제 항목에 대한 구현계획 수립 – 구현방법 정의 및 요구사항 파악 – 구현 책임자 및 자원 할당 – 구현일정 수립 등
		‣ 정보서비스 구성도 작성 – 보안통제 적용된 정보서비스 구성도

그림 2-13 보안대책 수립(Select) 단계의 주요활동 흐름도



1. 보안 요구사항 도출 [활동-4-1]

보안 요구사항 도출은 앞선 위협식별 단계의 모델 C/S/O 평가, 보안원칙 적용, 추가 위협식별(필요시) 등을 통해 식별한 보안위협에 대해서 차단, 예방, 탐지, 완화, 대응 등의 방어효과를 얻기 위한 요구사항을 도출하는 것을 말한다.

보안위협에 대한 적절한 보안 요구사항 도출을 위해서는 전문가 토론·설문·자문뿐만 아니라, ATT&CK 등 국제적으로 통용되는 다양한 보안 프레임워크를 이용할 수 있다.

또한, 보안 요구사항 도출 시에는 준비 단계에서 사전 설정한 정보서비스 보안목표(기초 보안 요구사항)를 포함한다.

2. 보안통제 선택 [활동-4-2]

앞서 도출된 보안 요구사항을 만족하는 구현 가능한 관리적·기술적 수단으로서 보안통제 항목을 선택하고 구현계획을 수립한다. 단, 보호대책을 적용하기 위한 방법으로 N2SF 보안통제 외에 관련 법령·규정 등에서 요구하는 추가적인 방안이 적용될 수도 있다.

다음 그림은 부록1(보안통제 항목 해설서)에 수록된 국가 망 보안체계 보안통제의 구조를 나타낸다. 보안통제 우선 검토사항은 C(기밀)·S(민감)·O(공개) 등급별 권고하는 보안통제 항목을 '●'로 표기하고 있으며, 국내 보안정책(국가정보보안기본지침, 각종 보안 가이드라인 등) 및 NIST SP 800-53B 등을 분석·최적화하였다. 사용제한을 권고하는 보안통제 항목은 '-'로 표기한다.

보안통제 항목을 선택하기 위해서는 ①보안통제 우선 검토사항을 활용하거나 ②정보서비스 모델 해설서(부록2)를 활용할 수 있다.

가. 보안통제 우선 검토사항 활용

국가 망 보안체계는 보안통제 우선 검토사항을 활용해 보안통제 항목을 선택할 수 있다. 업무정보 또는 정보시스템의 C/S/O 등급에 따라 '●' 표시가 되어있는 보안통제 항목을 선택할 수 있다.

보안통제 우선 검토사항은 업무정보·정보시스템 C/S/O 등급별 우선적으로 적용을 검토해야 하는 보안통제 항목으로 정보서비스 구성, 운용환경 및 기관 특성 등을 고려하여 보안통제 항목을 제외하거나 그 세부사항을 조정할 수 있다.

다음 그림은 O등급으로 분류된 업무정보·정보시스템에 대해서는 O등급 우선 검토사항 해당란에 '●' 표시가 되어있는 보안통제 항목을 우선적으로 선택하는 모습을 나타낸다.

그림 2-14 국가 망 보안체계 보안통제 항목 선택 방법(예: O등급 업무정보·정보시스템)



나. 정보서비스 모델 해설서 참조

정보서비스 모델 해설서(부록2)에 포함된 정보서비스 모델과 동일 또는 유사한 경우 해당 정보서비스 모델 구성요소에 대한 위협, 보안요구사항 등을 참조하여 보안통제 항목을 선정할 수 있다.

다. 보안통제 구현계획 수립

다음 표는 보안통제 구현계획 수립을 위한 활동을 나열한 것이다. 구현 우선순위 설정은 기관의 업무·기능 중요도 및 우선순위에 따라, 해당 업무·기능과 연계된 업무정보·정보시스템에 대한 보안통제 적용의 수준, 일정 등의 우선순위를 결정한다. 또한, 기관이 가진 인력·기술·예산 등의 상황도 함께 고려한다.

표 2-12 보안통제 구현계획 수립의 세부 활동

세부 활동	설명	비고
구현방법 정의 및 기술적 요구사항 파악	보안통제를 시스템에 구현·구축·운영하기 위한 구체적인 방법론, 절차, 기술적 요구사항(호환성 등) 정의	보안설정 적용, 보안기능 개발, 상용 보안 제품·서비스 도입 등
구현일정 수립	각 보안통제에 대한 구현일정 설정	구현 우선순위와 연계
구현 우선순위 설정	위협에 대한 위험평가 결과, 기관의 업무·기능 중요도 등에 따라 보안통제 우선순위 결정	
책임자 및 자원 할당	각 보안통제의 구현을 담당할 책임자를 지정하고, 통제구현에 필요한 인력, 기술, 예산 등을 배정	

제5절

적절성 평가·조정(Assess)

국가 망 보안체계의 전체 단계에서 요구되는 활동이 올바르게 이뤄졌는지 각 활동의 결과를 통해 평가하고 미흡한 점에 대해서는 조정하여 보완한다.

그림 2-15 적절성 평가조정 개념도

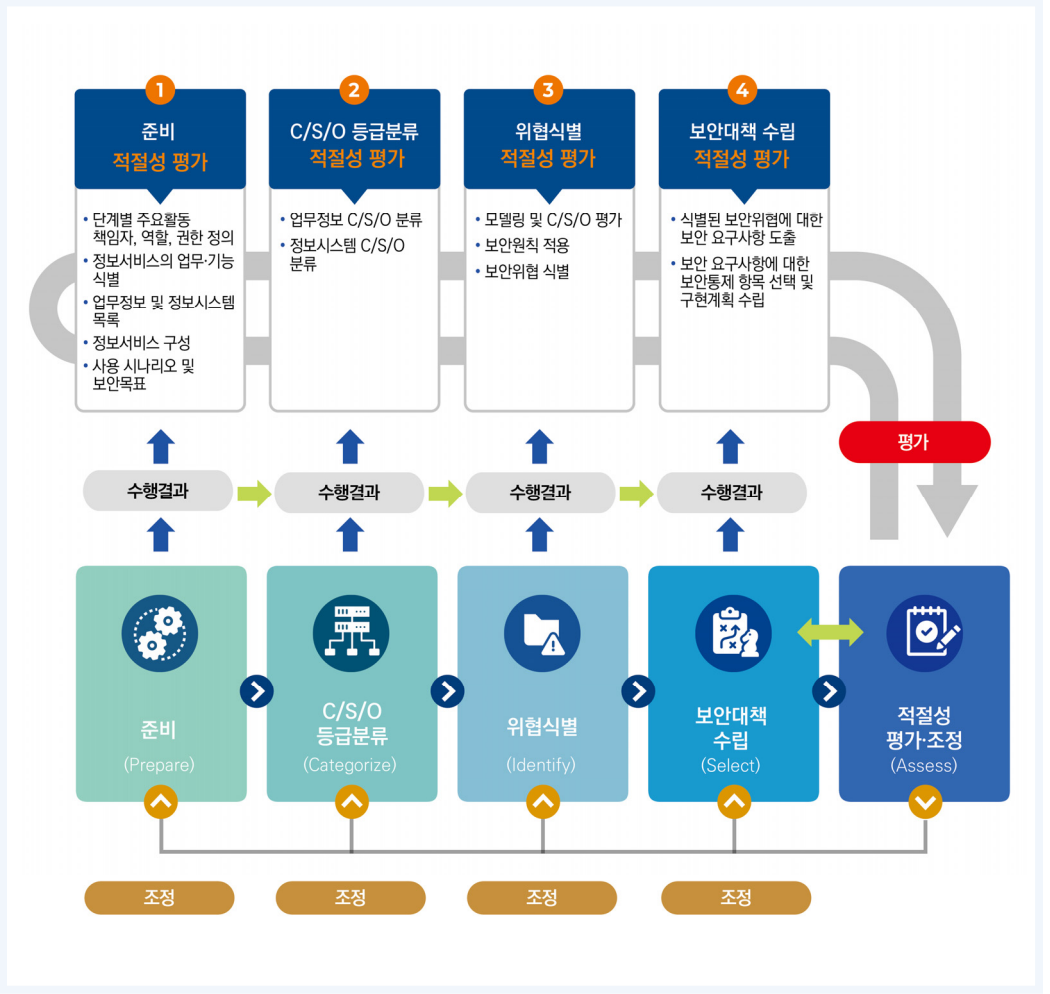


표 2-13 적절성 평가·조정(Assess) 단계 주요활동별 수행내용

단계	주요활동	수행내용
❺ 적절성 평가·조정 (Assess)	[활동-5-1] 적절성 평가	‣ 단계별 주요활동에서 생산된 중간 산출물, 자료, 지식 등을 토대로 적절성 평가기준에 따라 주요활동의 적절성 평가
	[활동-5-2] 적절성 평가결과 협의·조정	‣ 적절성 평가에서 '부적합'으로 평가된 평가항목에 대해 각 단계별 책임자와 협의 및 조정 - 문제점이 발견된 활동과 그에 영향받는 모든 활동 재수행 후 적절성 평가 재수행
	[활동-5-3] 적절성 평가결과 확인	‣ 적절성 평가에서 모든 평가항목이 '적합'으로 평가되며, 국정원 보안성 검토 의뢰를 위한 제반사항 준비완료 여부 확인 (정보보안담당관)

1. 적절성 평가 [활동-5-1]

국가 망 보안체계는 각 단계별 활동의 수행결과에 대해 각급기관이 자체적으로 적절성을 판단할 수 있도록 다음과 같은 평가지표를 권고한다.

단, 각 평가지표에 대한 세부적인 기준은 각급기관이 자율적으로 판단하며, 적절성 평가 결과는 기관이 자율적으로 관리할 수 있다.

가. 준비(Prepare) 단계에 대한 적절성 평가

표 2-14 준비(Prepare) 단계에 대한 적절성 평가지표

주요활동	평가지표 (권고)
[활동-1-1] N2SF 적용계획 수립	‣ 단계별 책임자 지정 및 역할·권한 정의는 기관의 규모, 역량 등을 충분히 고려하였는가?
	‣ 단계별 요구사항 정의, 수행일정 수립 등은 현실적으로 달성 가능한 수준인가?
[활동-1-2] 기관 업무·기능 분석	‣ 분석된 기관 업무·기능은 관련 정부기능분류체계, 지방기능분류체계, 지방교육기능분류체계 등 공공 BRM과 연계되는가? (무분별한 자체 BRM 수립 지양)
	‣ 분석된 기관 업무·기능은 BRM 기준 레벨5 이하로 세분화하였는가?
[활동-1-3] 업무정보 식별	‣ 본 정보화사업 범위에 해당하는 모든 업무정보가 적절한 수준으로 식별되었는가?

주요활동	평가지표 (권고)
[활동-1-4] 정보시스템 식별	▸ 식별된 업무정보의 생산, 저장, 처리, 이동, 보관, 폐기 등에 관여하는 정보시스템을 모두 식별하였는가?
[활동-1-5] 정보서비스 식별	▸ 네트워크, 정보시스템, 업무정보 등 정보서비스 구성 및 구조를 정확히 식별하였는가?
	▸ 정보서비스 목적과 용도에 따른 사용 시나리오를 적합하게 정의하였는가?
	▸ 정보서비스와 관련된 지침, 가이드라인 등을 참고하여 보안목표(기초 보안 요구사항)를 충분히 설정하였는가?

나. C/S/O 등급분류(Categorize) 단계에 대한 적절성 평가

표 2-15 C/S/O 등급분류(Categorize) 단계에 대한 적절성 평가지표

주요활동	평가지표 (권고)
[활동-2-1] 업무정보 C/S/O 등급분류	▸ 업무정보 C/S/O 등급분류 기준을 따르는가?
	▸ 준비단계에서 식별된 업무정보를 빠짐없이 분류하였는가?
[활동-2-2] 정보시스템 C/S/O 등급분류	▸ 업무정보와 정보시스템의 포함관계에 근거해 업무정보의 등급 중 최상위 등급을 정보시스템의 등급으로 분류하는가?
	▸ 하나의 정보시스템에는 가급적 동일 등급 업무정보로만 구성되도록 노력하였는가?

다. 위협식별(Identify) 단계에 대한 적절성 평가

표 2-16 위협식별(Identify) 단계에 대한 적절성 평가지표

주요활동	평가지표 (권고)
[활동-3-1] 모델링 및 C/S/O 평가	▸ 준비 단계에서 정의된 정보서비스 사용 시나리오별 「위치-주체-객체」 모델링 및 C/S/O 평가를 수행하였는가?
[활동-3-2] 보안원칙 적용	▸ 모델링 및 C/S/O 평가에서 보안등급 차이를 발견한 후 「정보 생산·저장」 및 「정보 이동」 원칙을 적용하였는가?
	▸ C/S/O 평가를 통해 보안등급의 차이가 발생하는 지점을 식별하였는가?
[활동-3-3] 보안위협 식별	▸ 「위치-주체-객체」 모델링 및 C/S/O 평가, 보안원칙 적용 등을 통해 서로 다른 보안등급 간 발생 가능한 정보서비스의 구조적 보안위협을 식별하였는가?
	▸ 취약점, 악성코드, DoS, 공급망보안, 내부자위협 등 다양한 보안위협을 식별하였는가?
	▸ 식별된 보안위협에 대한 위험평가를 수행하여 보안대책 적용이 필요한 위협을 선별하였는가?

라. 보안대책 수립(Select) 단계에 대한 적절성 평가

표 2-17 보안대책 수립(Select) 단계에 대한 적절성 평가지표

주요활동	평가지표 (권고)
[활동-4-1] 보안 요구사항 도출	▸ 준비단계에서 설정한 정보서비스 보안목표를 보안 요구사항에 포함하였는가?
	▸ 도출된 보안 요구사항은 해당 정보시스템 환경에 구현(개발, 제품도입 등) 가능한가?
[활동-4-2] 보안통제 선택	▸ 도출된 보안 요구사항을 만족하는 보안통제 항목을 적절히 선택하였는가?
	▸ C/S/O 등급에 따른 우선 검토사항(부록1 참조)을 반영하였는가?
	▸ N2SF 기본 보안통제 항목(부록1 참조)에 적절한 항목이 없는 경우 기관이 자체적으로 보안통제 항목을 정의하였는가?
	▸ 보안통제 항목에 대한 구현계획이 구체적으로 수립되었는가?
	▸ 보안통제 항목 구현계획에 구현방법 및 요구사항이 명확하게 포함되었는가?

2. 적절성 평가결과 협의·조정 [활동-5-2]

단계별 적절성 평가 결과 부적합 항목이 발견되는 경우 해당 활동이 포함된 단계와 그 이후 단계의 활동을 재수행토록 해당 단계의 책임자와 협의·조정한다. 단, 재수행되는 활동으로 인해 영향받는 다음 단계의 활동만 재수행하도록 그 범위를 제한하여 재수행에 따른 업무 부담을 경감시킨다.

그림 2-16 조정 대상 단계에 따른 절차별 활동 재수행 개념 및 범위(C/S/O 등급분류 조정 예시)



3. 적절성 평가결과 확인 [활동-5-3]

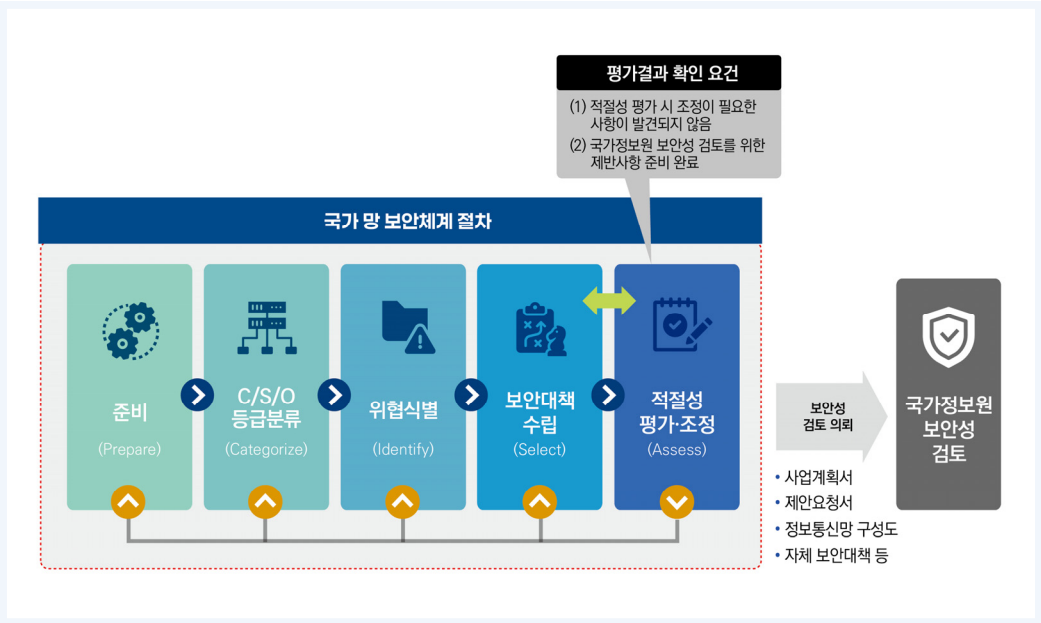
적절성 평가 및 협의·조정이 완료된 후, 적절성 평가결과에 대한 최종 확인은 정보보안담당관에 의해서 이뤄지며 다음 두 가지 조건을 모두 만족하는 경우에만 가능하다.

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 확인을 국가정보원 보안성 검토와 연계되도록 한다.

그림 2-17 적절성 평가결과 확인 요건





국가 망 보안체계
보안 가이드라인

제3장

산출물 및 보안성 검토

제1절 단계별 주요활동 요약

제2절 보안성 검토 시 제출하는 최종 산출물

제1절

단계별 주요활동 요약

다음 표는 국가 망 보안체계의 5단계 주요활동 수행내용을 요약하여 정리한 것이다. 각 단계별 수행결과는 각급기관이 자율적으로 관리·활용하고, 전체 단계의 수행결과를 종합한 최종 산출물(자체 보안대책, 별도 서식 참고)은 국가정보원 보안성 검토 시에 제출한다.

표 3-1 단계별 주요활동 요약

단계	주요활동	수행내용
❶ 준비 (Prepare)	[활동-1-1] N2SF 적용계획 수립	▸ 단계별 책임자 지정 및 역할·권한 정의 – 적절성 평가·조정 단계 책임자는 정보보안담당관으로 지정
		▸ 단계별 요구사항 정의, 수행일정 수립 등
	[활동-1-2] 기관 업무·기능 분석	▸ 본 정보화사업 범위에 해당하는 정부기능분류체계, 지방기능분류체계, 지방교육기능분류체계 등에 따른 기관업무·기능 분석을 통해 BRM 연계 – 정보서비스 업무·기능 식별 (레벨5 이하 권고)
	[활동-1-3] 업무정보 식별	▸ 본 정보화사업 범위에 해당하는 정보서비스의 업무·기능 수행시 생산, 저장, 처리, 이동, 보관, 폐기되는 업무정보 식별 – 기관 업무·기능에 대한 업무정보 관계 파악
	[활동-1-4] 정보시스템 식별	▸ 업무정보의 생산, 저장, 처리, 이동, 보관, 폐기에 관여하는 정보시스템 식별 – 정보시스템의 물리적·논리적 구성, 업무정보 관련성 등 파악
	[활동-1-5] 정보서비스 식별	▸ 네트워크, 정보시스템, 업무정보 등 정보서비스 구성 및 구조 분석
		▸ 정보서비스 목적과 용도에 따른 사용 시나리오 정의 – 1개 이상의 사용 시나리오 가능
		▸ 정보서비스의 보안목표(기초 보안 요구사항) 설정 – 정보서비스 사용 시나리오 고려 – 관련 지침, 가이드라인 등 참고
❷ C/S/O 등급분류 (Categorize)	[활동-2-1] 업무정보 C/S/O 등급분류	▸ 업무정보의 C/S/O 등급분류 – 준비 단계에서 식별된 업무정보에 대한 C/S/O 등급분류
	[활동-2-2] 정보시스템 C/S/O 등급분류	▸ 업무정보의 생산·저장·처리·이동·보관·폐기 등에 관여하는 정보시스템의 C/S/O 등급분류

단계	주요활동	수행내용
❸ 위협식별 (Identify)	[활동-3-1] 모델링 및 C/S/O 평가	▸ 정보서비스 사용 시나리오에 대한 「위치-주체-객체」 모델링 및 C/S/O 평가를 통해 보안등급 차이에 따른 보안대책 필요 여부 판단
	[활동-3-2] 보안원칙 적용	▸ 정보서비스 사용 시나리오별 「위치-주체-객체」 모델을 기반으로 「정보 생산·저장」 및 「정보 이동」 상황에서의 보안등급 차이에 따른 보안대책 필요 여부 판단 및 보안대책 적용지점 식별
	[활동-3-3] 보안위협 식별	▸ 「위치-주체-객체」 모델링 및 C/S/O 평가, 보안원칙 적용 결과를 기반으로 서로 다른 보안등급 간 발생 가능한 보안위협 식별
❹ 보안대책 수립 (Select)	[활동-4-1] 보안 요구사항 도출	▸ 식별된 보안위협에 대한 보안 요구사항 도출 - 기관의 특성, 업무정보·정보시스템·정보서비스 특성 등에 따라 다양하게 도출 가능 - 준비단계에서 설정한 정보서비스 보안목표를 보안 요구사항에 포함 - 보안위협과 보안 요구사항의 관계는 1:1, 1:N, N:1 가능
	[활동-4-2] 보안통제 선택	▸ 도출된 보안 요구사항을 만족하는 물리적·관리적·기술적 수단으로서의 보안통제 항목 선택 - C/S/O 등급에 따른 우선 검토사항 고려 - N2SF 기본 보안통제 항목 외에 추가적인 보안통제 항목을 각급기관이 자체적으로 정의하여 사용 가능 - 정보서비스 보안목표, 업무정보·정보시스템·정보서비스 특성, 보안통제 특성 등에 따른 세부사항 조정 가능
		▸ 보안통제 항목에 대한 구현계획 수립 - 구현방법 정의 및 요구사항 파악 - 구현 책임자 및 자원 할당 - 구현일정 수립 등
		▸ 정보서비스 구성도 작성 - 보안통제 적용된 정보서비스 구성도
❺ 적절성 평가·조정 (Assess)	[활동-5-1] 적절성 평가	▸ 단계별 주요활동에서 생산된 중간 산출물, 자료, 지식 등을 토대로 적절성 평가기준에 따라 주요활동의 적절성 평가
	[활동-5-2] 적절성 평가결과 협의·조정	▸ 적절성 평가에서 '부적합'으로 평가된 평가항목에 대해 각 단계별 책임자와 협의 및 조정 - 문제점이 발견된 활동과 그에 영향받는 모든 활동 재수행 후 적절성 평가 재수행
	[활동-5-3] 적절성 평가결과 확인	▸ 적절성 평가에서 모든 평가항목이 '적합'으로 평가되며, 국정원 보안성 검토 의뢰를 위한 제반사항 준비완료 여부 확인 (정보보안담당관)

제2절

보안성 검토 시 제출하는 최종 산출물

1. 국가 망 보안체계를 통한 보안성 검토

각급기관이 추진하는 정보화사업에 대해서 국가정보원 보안성 검토 시 제출하는 문서는 ①사업계획서, ②제안요청서, ③정보통신망 구성도, ④자체 보안대책 등 총 4종이다.

①사업계획서 및 ②제안요청서에는 해당 정보화사업에 대한 기본적인 설계, 구축 뿐만 아니라 국가 망 보안체계(N2SF) 5단계 절차 수행을 통해서 도출된 보안통제를 구현(제품도입, 개발 등)하기 위한 세부내용, 계획 등이 포함된다.

③정보통신망 구성도에는 국가 망 보안체계 수행을 통해서 도출된 보안통제가 적용된 네트워크 구조를 반영하게 된다.

④자체 보안대책은 국가 망 보안체계 5단계 주요활동의 결과를 종합한 최종 산출물(별도 서식 참고)을 활용할 수 있다.

표 3-2 국가 망 보안체계 수행결과를 이용한 보안성 검토

보안성 검토 시 제출문서	국가 망 보안체계(N2SF) 수행결과 반영	비고
① 사업계획서	정보화사업에 대한 기본적인 설계, 구축뿐만 아니라 국가 망 보안체계를 통해 수립한 보안통제의 구현(제품도입, 개발 등)에 관한 세부내용 및 계획 포함	
② 제안요청서		
③ 정보통신망 구성도	국가 망 보안체계를 통해 수립한 보안통제가 적용된 네트워크 구조 반영	
④ 자체 보안대책	국가 망 보안체계의 단계별 주요활동 수행결과를 종합한 최종 산출물	별도 서식 참고

2. 최종 산출물 서식

■ 국가 망 보안체계 보안 가이드라인 1.0 (최종 산출물 서식)

자체 보안대책

1. 정보서비스 보안목표 (규정·지침 등에 따른 기초 보안 요구사항)

번호	구분	보안목표	비고
1	*네트워크*	*기관 업무영역과 구분되는 별도의 연구망 구성하여 연구망 침해 시 피해 전이 방지*	
2		*연구목적에 필요한 인터넷 서비스만 접속*	
3	*연구단말*	*인터넷과 연구시스템 동시연결 차단*	

2. C/S/O 등급분류

번호	정보시스템		업무정보		비고
	명칭	C/S/O 등급	명칭	C/S/O 등급	
1	*연구단말*	*S*	*인터넷 수집자료*	*O*	
			인터넷 수집자료 취합 문서	*S*	
2	*연구시스템*	*S*	*연구 보고서*	*S*	
			SW 설계서 및 소스코드	*S*	
			시험개발용 SW	*S*	

3. 보안 요구사항 및 보안통제

번호	보안위협 발생지점	보안 요구사항	보안통제 항목 (부록1)	비고
1	*연구단말*	*인터넷 사용 시, 연구시스템 사용 시 작업공간 및 네트워크 분리*	*N2SF-...*	
		정보흐름 통제(인터넷->연구단말->연구시스템만 허용)	*N2SF-...*	
2	*연구단말*	*연구보고서 DRM 적용*	*N2SF-...*	
3	*연구단말*	*승인받은 지정 단말만 접속 허용*	*N2SF-...*	
4	*연구시스템*	*최신버전 SW 적용*	*자체-1*	*부록1(보안통제 항목 해설서)에 없는 보안 통제 추가 적용*
		보안패치 관리	*자체-2*	
5	*연구시스템*	*다중요소인증(MFA)*	*N2SF-...*	

4. 보안통제 구현계획

번호	보안통제 항목	적용 대상	보안통제 적용 방안	보안통제 구현·운영 요건	비고
1	*N2SF-...* *N2SF-...*	*연구시스템*	*OOO 솔루션 도입*	*기존 도입 관련 제품과 호환성 유지*	
2	*N2SF-...* *N2SF-...* *N2SF-...*	*인터넷 연계구간*	*SW 개발 용역*	*SW 개발보안 가이드라인 적용 및 소스코드 보안약점 분석도구 적용*	
3	*자체-1*	*연구시스템*	*운영체제 보안설정 적용 강제화*	*매월/수시 적용여부 확인*	



국가 망 보안체계
보안 가이드라인

참고

제1절 주요국 보안정책 동향

제2절 N2SF 오버레이 개념을 통한 절차·원칙 통합 보안체계

제3절 CDS(Cross Domain Solution)

제1절

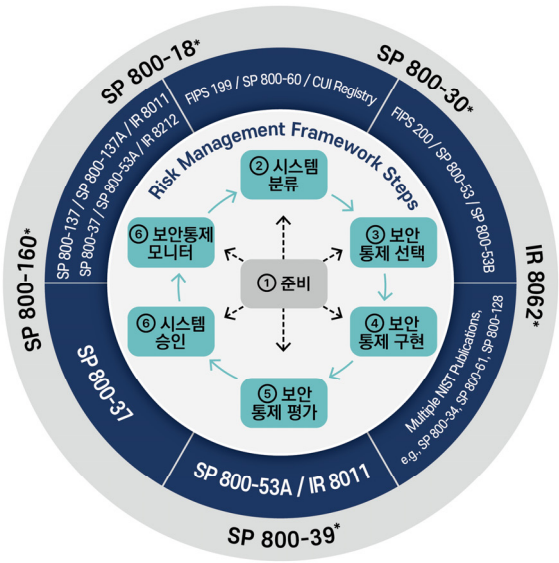
주요국 보안정책 동향

1. 미국 NIST RMF (Risk Management Framework)

미국 연방기관은 연방정보보안관리법(FISMA) 및 관리예산실(OMB) 회람 A-130에 따라 정보시스템을 관리할 때 국립표준기술원(NIST)에서 정의한 위험관리체계(NIST RMF) 및 보안통제(NIST SP 800-53)를 준수하고 있다.

NIST RMF는 정보보안 및 개인정보보호를 위한 위험관리 프레임워크로 위험관리, 위험평가, 보안분류, 보안통제, 지속 모니터링 및 평가 등에 관한 세부적인 지침을 다루고 있으며, 민간 기업도 NIST RMF를 적용하는 추세이다. 특히 국방, 에너지, 의료, 금융 등 고위험 산업 분야는 정보시스템 보호를 위해 정보보호 지침 및 통합 보안 방안으로 폭넓게 활용되고 있다.

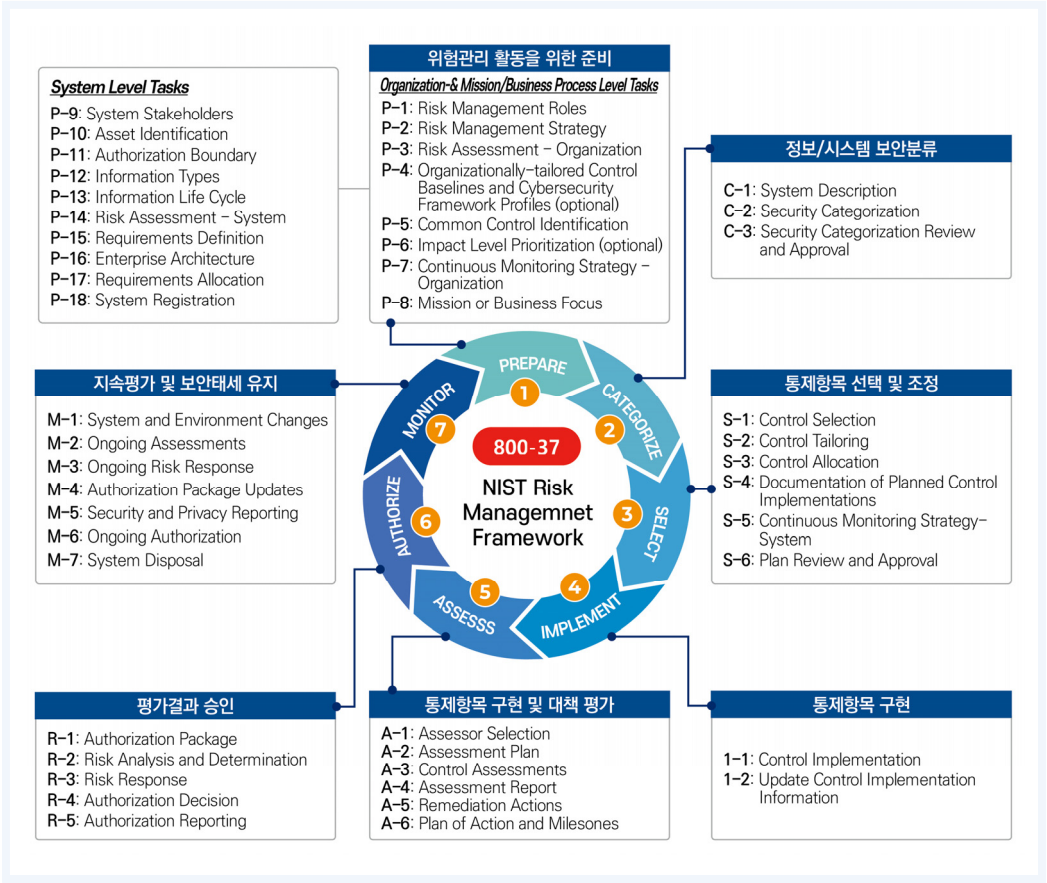
그림 참고-1 NIST RMF를 구성하는 관련문서(가이드라인) 목록



NIST RMF는 ①준비, ②시스템 분류, ③보안통제 선택, ④보안통제 구현, ⑤보안통제 평가, ⑥시스템 승인, ⑦보안통제 모니터 등의 7단계 절차로 구성되며 지속적인 보안강화를 위해 순환하는 개념을 가지고 있다.

각 단계별 주요활동은 관련 문서(가이드라인)를 참고하여 활동을 수행한다.

그림 참고-2 NIST RMF의 위험관리를 위한 각 단계 주요활동



2. 영국 GSCP (Government Security Classifications Policy)

2014년 영국 정부가 수립한 GSCP(Government Security Classifications Policy, 정부 보안분류 정책)는 정보를 OFFICIAL, SECRET, TOP SECRET 세 가지 등급으로 분류하고 등급별

서로 다른 보안 요구사항을 갖는다. 각 등급은 정보 노출 시 국가안보, 경제적 이익, 국제 관계에 미칠 수 있는 피해의 심각성에 따라 결정된다.

표 참고-1 영국 GSCP(Government Security Classifications Policy) 개요

구분	정의	보안 요구사항
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

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

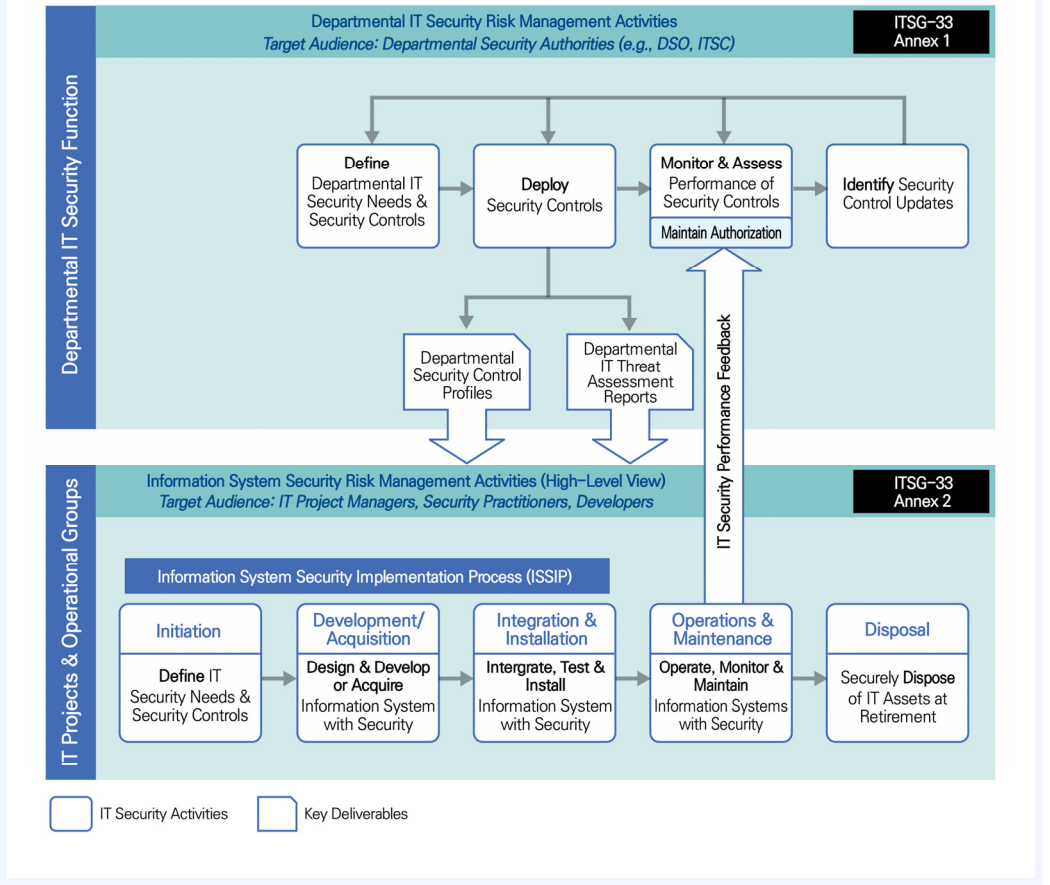
캐나다 ITSG-33은 NIST RMF를 바탕으로 캐나다 정부의 요구사항을 충족하도록 개발되었다. 2009년 캐나다 정부의 보안정책에 따라 2010년 위험관리 프레임워크의 기본 틀을 개발한 후 2012년 프레임워크를 구체화한 기본 가이드라인을 발표했다.

표 참고-2 캐나다 ITSG-33 연혁

년도	구분	관련문서 (지침 및 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

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

그림 참고-3 캐나다 ITSG-33 구조



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.

4. 호주 ISM (Information Security Manual)

호주 ISM(정보보안 매뉴얼)은 ISO/IEC 27001(ISMS)을 기반으로 정부 기관의 정보보안 가이드라인을 제공하며 거버넌스, 식별, 보호, 탐지, 대응의 영역으로 구성된다.

표 참고-3 호주 ISM(정보보안매뉴얼) 구조

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
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 시스템 간 이동 시 암호화
	Protect-8	다른 시스템 간 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

제2절

N2SF 오버레이 개념을 통한 절차·원칙 통합 보안체계

N2SF에서 제시하는 오버레이(Overlay) 개념은 국가 망 보안체계가 규정한 기본 보안통제 항목을 단순히 일괄 적용하는 것이 아니라, 각 기관의 운영 환경과 위협 수준, 정책 요구사항, 그리고 최신 보안 전략을 반영하여 맞춤형 보안통제 집합으로 재구성·적용하는 방식을 의미한다. 이는 미국의 NIST 위험관리 프레임워크(RMF)에서 정의한 오버레이 개념과 궤를 같이하는 것으로, 공통적으로 따라야 하는 보안통제 기준선(Baseline, 우선 검토사항)을 유지하면서도 각 기관별 상황에 적합한 보안통제를 '덧씌우는' 접근이라고 할 수 있다. 즉, 오버레이는 획일적 보안기준이 아니라 공통성과 특수성을 동시에 반영하는 탄력적 장치라 볼 수 있다.

이러한 접근은 해외에서도 이미 활용되고 있다. 대표적인 사례가 미국 국방부의 제로트러스트 오버레이(DoD ZT Overlay)이다. 국방부는 NIST SP 800-53의 표준 보안통제 체계에 제로트러스트 원칙(최소 권한, 지속적 검증, 데이터 중심 보호, 자산 기반 보안 등)을 덧씌워 새로운 통제 집합을 구성하고, 이를 자국 국방 네트워크 전반에 적용을 추진하고 있다. 즉, 기존 통제만으로는 대응하기 어려운 최신 위협 환경을 보완하기 위해, 오버레이 방식을 통해 기존 체계를 대체하지 않고 강화한 것이다.

N2SF도 이와 유사하게, 각 기관이 보안대책을 수립할 때 단순히 통제 목록을 따르는 수준에 머무르지 않고 제로트러스트 원칙이나 기관 고유의 임무 특성을 고려하여 통제를 재해석하거나 세분화할 수 있는 여지를 제공한다. 따라서 N2SF에서의 오버레이는 제도적 통일성과 기관별 자율성을 동시에 담보하는 확장 레이어라 할 수 있으며, 이는 반드시 N2SF가 규정한 절차와 각 통제 목표를 준수하는 범위 내에서 활용되어야 한다.

N2SF가 제시하는 5단계 절차(준비 – C/S/O 등급분류 – 위협식별 – 보안대책 수립 – 적절성 평가·조정)는 RMF가 보여주는 절차적 구조와 유사하다. 그러나 단순히 형식적 절차를 따르는 데 그치지 않고 제로트러스트의 철학을 동시에 포용한다는 점에서 차별성이 있다. 제로트러스트는

독립된 단계가 아니라 보안대책 수립 단계에서 핵심 원칙으로 적용된다. 위협을 식별한 이후 대응 방안을 마련하는 과정에서 '항상 검증(Always Verify)'과 '최소 권한(Least Privilege)' 원칙을 통제 설계에 반영함으로써, 기존 보안통제의 실행력을 강화하고 지속적인 보안 확보가 가능하다.

또한 N2SF 부록1(보안통제 항목 해설서)에 제시된 6개 대항목 분류는 제로트러스트의 핵심 구성요소인 필러(Pillar)와 직접적으로 대응된다. 이러한 대응 관계는 N2SF가 제로트러스트 아키텍처를 수용할 수 있는 구조적 기반을 제공함을 보여준다. 즉, N2SF는 RMF 기반의 절차 중심 보안관리 체계와 제로트러스트 아키텍처 기반 보안원칙을 오버레이 함으로써, 통합형 보안체계로 자리매김할 수 있다.

아울러 제로트러스트의 성숙도 모델은 N2SF의 보안통제 항목 적용 절차와 연계할 수 있다. N2SF의 기준선은 기관이 확보해야 할 최소한의 필수 보안통제로 설정되며, 이를 기반으로 위협 환경이나 업무 특성을 고려해 점진적으로 확장하도록 설계한다. 이는 제로트러스트가 성숙도 모델에 따라 단계적으로 발전해나가는 방식과 대응된다. 따라서 기준선 검토를 통해 제로트러스트 원칙이 제도적으로 구현될 수 있으며, 점진적·지속적 보안 강화로 이어질 수 있다.

결과적으로 N2SF는 미국의 RMF와 같이 검증된 절차적 보안관리 구조를 갖추는 동시에, 글로벌 보안 트렌드인 제로트러스트의 원칙을 유연하게 수용할 수 있는 통합형 국가 보안체계로 평가된다. 이러한 구조 덕분에 N2SF는 공공기관이 공통적으로 따라야 할 최소 기준을 명확히 제시하면서도, 기관별 환경에 맞춰 최신 보안 전략을 탄력적으로 반영·재구성할 수 있는 융통성을 제공한다. 이는 곧 "제도적 일관성"과 "전략적 유연성"을 동시에 달성하려는 국가 보안정책의 방향성과도 부합한다.

제3절

CDS(Cross Domain Solution)

미국은 NSA 산하 국가크로스도메인전략관리국(NCDSMO: National Cross Domain Strategy & Management Office)을 중심으로 연방정부, 국방부, 동맹국 등과의 정보공유에 필요한 CDS 체계를 통합적으로 관리·감독하는 업무를 수행하고 있다. 이를 통해 국가 CDS 체계에 대한 기술정책 수립, 보안 위협 모델 및 보안 요구사항 도출, 침투시험 등을 토한 평가 검증을 수행하여 서로 다른 보안도메인간의 연계기술을 주도하고 있다.

국가 망 보안체계(N2SF)는 망 분리 중심에서 AI 등 신기술 융합 및 데이터 공유·활용 중심의 정보보안 체계로 전환하기 위해 업무정보를 C/S/O 등급으로 분류하여 차등적인 보안통제를 적용한다. 이때 분류된 데이터는 보안수준이 서로 다른 등급의 보안도메인에 존재할 수 있으며, 안전한 데이터 활용 및 보호를 위해서는 데이터 연계 구간에서의 보안통제 기술이 필요하다.

CDS는 상이한 등급의 보안도메인 환경에서 각 도메인 내부를 위협으로부터 보호하면서 다른 도메인으로 데이터를 검증된 방식으로 안전하게 전달한다. 업무자료의 보안등급 및 업무환경에 따라 도메인 간 물리적·논리적으로 분리하거나 DLP·CDR·ABAC 등을 통해 정보 흐름을 통제할 수 있다.

CDS는 기능과 목적에 따라 접근 CDS(Access CDS), 전송 CDS(Transfer CDS), 다중등급보안 CDS(Multi Level Security, MLS CDS) 등으로 세분화할 수 있다. N2SF 환경에서 데이터의 등급, 정보 흐름의 방향성, 업무의 성격에 따라 최적의 CDS 유형을 선택할 수 있다.

1. 접근 CDS (Access CDS)

접근 CDS는 사용자가 단일 업무단말로 보안등급이 서로 다른 여러 보안도메인에 접속 가능하지만, 도메인 간 데이터 전달은 통제하는 방식이다. 사용자는 데이터를 직접 옮기지 않고도 필요한 자원에 접근해 실시간으로 업무를 처리할 수 있다.

업무망의 사용자가 업무상 필요에 의해 인터넷망의 웹사이트나 데이터베이스에 안전하게 접근해야 할 경우, 접근 CDS는 가상화 기술 등을 이용해 서로 다른 보안등급에서 화면 정보만을 안전하게 중계하여 열람 및 활용이 가능하다. 이를 통해 불필요한 파일 다운로드를 최소화하고 정보 유출 위협을 줄일 수 있다.

2. 전송 CDS (Transfer CDS)

전송 CDS는 보안등급이 서로 다른 보안도메인 간에 업무정보를 안전하게 전달하기 위해 망 또는 정보시스템 경계 지점에서 운영하는 방식이다. 자료 전송 방식에 따라 단방향(One-way)과 양방향(Two-way) 기술 방식으로 나뉜다.

단방향 전송 CDS는 물리적으로 데이터가 한쪽으로만 흐르도록 설계되어, 외부로부터의 위협이 내부망으로 유입되는 것을 원천 차단하는 기술이다. 업무망에서 생산된 데이터를 인터넷망으로 전송할 때, 데이터 유출이나 악성코드 유입 가능성을 제거하여 내부망을 보호한다.

양방향 전송 CDS는 정해진 프로토콜과 정책에 따라 양방향으로 데이터를 주고받되, 전송되는 모든 파일과 콘텐츠의 무결성을 검사하고 악성코드를 탐지·차단하는 필터링 기능을 내장한다. 인터넷망에서 수신한 공개 정보를 악성코드 검사 후 안전하게 업무망으로 전달하거나, 업무망의 파일을 보안 심사 후 외부로 전송하는 등의 업무에 활용된다.

3. 다중등급보안 CDS (MLS CDS)

다중등급보안(Multi Level Security, MLS) CDS는 단일 업무시스템 내에 여러 보안등급의 업무정보가 존재할 때 사용자별 보안등급에 따라 접근할 수 있는 업무정보를 통제한다. 데이터 자체에 보안등급을 부여하고 이를 기반으로 정보 흐름 및 데이터 송·수신을 제어한다.

국방·외교 등 안보분야에서 여러 등급의 정보를 종합하여 상황을 판단하고 의사결정을 내려야 할 때 MLS CDS가 활용될 수 있다. 보안등급이 높은 사용자는 기밀정보와 민감·공개 정보를 함께 접속할 수 있지만, 등급이 낮은 사용자는 동일 시스템에 접근하더라도 공개 또는 민감정보만 볼 수 있도록 통제한다.

주요 용어 및 약어

1. 용어

용어	의미	비고
정보화사업	▸ 각급기관에서 정보통신망 또는 정보시스템을 개발·구축·운용·유지보수하는 사업 ▸ 정보화사업을 담당하는 정보화사업담당관은 해당 정보화사업에 대한 보안관리를 수행하여야 한다	국가정보보안기본지침 제11조(보안책임)
정보보안, 사이버보안	▸ 각급기관의 기능 유지를 주(主)목적으로 정보통신망 및 정보시스템을 통해 수집, 가공, 저장, 검색, 송·수신되는 정보의 유출, 위·변조, 훼손 등을 방지하기 위하여 관리적·물리적·기술적 수단을 강구하는 일체의 행위	국가정보보안기본지침 제2조(정의)
	▸ 사이버 환경에서 네트워크를 통해 연결된 조직·사용자 자산을 보호하기 위해 사용되는 기술적 수단, 보안정책, 개념, 보안 안전장치, 가이드라인, 위기관리방법, 보안 행동, 교육·훈련, 모범사례, 보안 보증, 그리고 보안 기술들의 집합	정보보호 기술 용어 (TTAK.KO-12.0002/R3, 2023.12. 개정)
업무정보, 업무자료	▸「전자정부법」 제2조제6호에 따른 행정정보, 「전자정부법」 제2조제6호에 따른 전자문서, 「공공기록물 관리에 관한 법률 시행령」 제2조제2호에 따른 전자기록물, 기타 다른 법령에 의하여 공무원 등이직무상 작성·취득하였거나 보유·관리하는 자료로서 전자적으로 처리되어 부호·문자·음성·음향·영상 등으로 표현된 것	국가정보보안기본지침 제2조(정의)
내부망	▸ 각급기관의 장이 기관의 업무 수행을 위하여 인터넷과 별도로 분리하여 구축한 업무 전용(專用) 정보통신망	국가정보보안기본지침 제2조(정의)
기관 인터넷망	▸ 각급기관의 장이 소속 공무원 등의 업무 활용 또는 공개서버 운용을 주목적으로 인터넷과 연동하여 구축한 정보통신망	국가정보보안기본지침 제2조(정의)
상용 인터넷망	▸ 각급기관의 장이 기관 인터넷망과 별개로 소속 공무원 등이나 민원인 등의 보편적인 편의성을 위하여 인터넷에 연동하여 구축한 정보통신망	국가정보보안기본지침 제2조(정의)
정보시스템	▸ 정보의 수집·가공·저장·검색·송신·수신 및 그 활용과 관련되는 기기와 소프트웨어의 조직화된 체계	TTA 정보통신용어사전
		국가정보보안기본지침 제2조(정의)
		「전자정부법」 제2조 제13호

용어	의미	비고
정보서비스	▸ 업무정보를 이용해 특정 서비스를 제공하기 위해 하나 이상의 정보시스템으로 구성된 체계 ▸ 정보화사업에서 정보시스템은 구축 및 운영의 대상이며, 정보시스템을 통해서 정보서비스를 제공	
위협, Threat	▸ 자산에 손실을 발생시키는 원인이나 행위 ▸ 보안에 해를 끼치는 행동이나 사건	TTA 정보통신용어사전
위험, Risk	▸ 예상되는 위협 때문에 자산에 발생할 가능성이 있는 손실의 기대치 ▸ 자산의 가치 및 취약성과 위협 요소의 능력, 보호 대책의 효과 등에 의해 영향을 받는다	TTA 정보통신용어사전
위험분석, Risk Analysis	▸ 보안 위험을 확인하고 그것들의 중요도를 결정하며 보호수단을 요하는 부분을 확인하는 과정 ▸ 정보시스템과 관련 자산의 기밀성, 무결성, 가용성에 영향을 미칠 수 있는 다양한 위협에 대해 시스템이 취약함을 인식하고, 이로 인해서 예상되는 손실을 분석하며, 안전한 정보시스템을 구현하고, 정보자원에 대한 위험요소를 식별, 평가하여 그러한 위험요소를 적절하게 통제할 수 있는 수단을 체계적으로 구현하고 운영하는 전반적인 행위 및 절차로서 위험분석은 위험관리의 일부분이다	TTA 정보통신용어사전
위험평가, Risk Assessment	▸ 정보시스템 관련 자산의 위험 분석을 통해 확인된 보안위협 요소와 위협 요소를 통해 발생 가능한 손실 정도를 추정하는 방법 ▸ 위험평가 결과에 따른 우선순위에 의거하여 보안대책이 수립된다	TTA 정보통신용어사전
위험관리, Risk Management	▸ 정보시스템 자산에 피해를 끼칠 수 있는 위협의 영향을 확인, 통제, 제거, 최소화하는 전체 과정. 위험 분석, 위험의 처리에 대한 결정, 보호 대책의 선정 및 구현, 잔여 위험 분석 등을 포함하는 순환적 과정으로 이루어진다.	TTA 정보통신용어사전
위협모델링, Threat Modeling	▸ 시스템에 대한 위협을 식별하고 이를 예방하거나 위협으로 인해 야기되는 악영향을 완화하는 보안대책을 정의하는 보안강화 활동	OWASP
	▸ a family of activities for improving security by identifying threats, and then defining countermeasures to prevent, or mitigate the effects of, threats to the system	
보안통제, Security Control	▸ 정보시스템을 보호하기 위해 제공된 하드웨어, 펌웨어 및 소프트웨어 안에서 구현되는 보안 메커니즘과 물리적, 인적, 절차적 및 관리적 보안 요구 사항을 포함하는 조치 사항들	정보보호 기술 용어 (TTAK.KO-12.0002/ R3, 2023.12. 개정)
	▸ 보안정책을 실현하기 위해 필요한 요구사항이나 준수사항을 언급한 일련의 규칙	안전한 소프트웨어 운용을 위한 지침 (TTAS.KO-10.0073/ R1, 2006.12. 개정)
	▸ 위험을 제거하거나 수용 가능한 수준으로 경감시킬 수 있는 보안대책으로 물리적, 관리적, 기술적 보안통제 등으로 구분됨	

용어	의미	비고
사용 시나리오	▸ 시스템의 행위에 대한 액터(실행자)와 시스템간의 상호작용에 대하여 정의한 것	시스템 통합 절차 지침 (TTAS.KO-10.0140, 2003.10. 제정)
	▸ 시스템이 수행하는 일련의 조치사항(sequences of actions)들을 설명한 것 ▸ 시스템이 이들 조치사항을 수행함으로써 행위자에게 가시적인 결과를 제공	소프트웨어 컴포넌트 용어 표준 (TTAS.KO-11.0029, 2003.10. 제정)
	▸ 정보서비스가 제공하는 기능을 이용해 기관의 업무를 수행하는 과정 및 시나리오	
기능분류	▸ 중앙행정기관(대통령 및 국무총리 소속기관을 포함하며, 이하 "행정기관"이라 한다)의 업무 및 그와 관련된 정보를 체계적으로 관리·활용하기 위하여 행정기관의 업무를 기능 중심으로 분류하는 것	정부기능의 분류 및 관리에 관한 규정 제2조 (정의)
기록관리기준표, BRM (Business Reference Model)	▸ 2007년 『공공기록물 관리에 관한 법률』이 개정되면서 업무에 기반한 기록관리 체계를 구축하기 위하여 "기록물분류기준표" 제도를 대체할 정부기능분류체계(BRM: Business Reference Model)를 기록분류체계로 도입하여 "기록관리기준표" 제도를 운용 ▸ 기록관리기준표 제도는 2008년에는 중앙행정기관에서 도입·운영하였으며, 이후 지방자치단체, 교육청 등으로 도입·운영	공공기록물 관리에 관한 법률
크로스도메인솔루션 CDS (Cross Domain Solution)	▸ 분리된 시스템이나 네트워크(이를 보안 도메인이라 부른다)는 서로 다른 유형의 위협과 위험 수준에 노출될 수 있으므로, 이를 다루기 위해 서로 다른 보안 정책을 가질 수 있다. 이러한 환경에서 CDS는 서로 다른 보안등급을 가진 도메인 간에 정보를 수동 또는 자동으로 접근하고 전송할 수 있도록 하는 제어된 인터페이스 형태이다. CDS는 하나 이상의 장치로 구성될 수 있다.	NIST SP 800-53 Rev.5(참조)
제로트러스트, Zero Trust	▸ 조직 네트워크 내·외부에 있는 모든 주체가 신뢰 영역으로 간주되는 조직 내부 네트워크의 자원 또는 데이터에 접근할 때 강한 인증, 정교한 접근 통제 그리고 지속적 모니터링 등을 통해 신뢰할 수 있는 이용자인지 지속적으로 검증·확인함으로써 위험을 완화하는 새로운 보안 프레임워크	TTA 정보통신용어사전

2. 약어

- **AI** Artificial Intelligence
- **ATT&CK** Adversarial Tactics, Techniques and Common Knowledge
- **BRM** Business Reference Model
- **CISO** Chief Information Security Officer
- **CDS** Cross Domain Solution
- **CTI** Cyber Threat Intelligence
- **DoS** Denial of Service
- **ICT** Information and Communication Technology
- **MLS** Multi Level Security
- **N2SF** National Network Security Framework
- **NIST** National Institute of Standards and Technology
- **OWASP** The Open Worldwide Application Security Project
- **ZT** Zero Trust

참고 문헌

[1] Adam Shostack, “Threat Modeling: Designing for Security”, John Wiley & Sons Inc., ISBN: 9781118809990, 2014. 2.

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

[3] FIPS 199, Standards for Security Categorization of Federal Information and Information Systems, 2004. 2.

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

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

[6] Guidance 1.2 – Working at SECRET, Cabinet Office, 2024. 8.

[7] Guidance 1.3 – Working at TOP SECRET, Cabinet Office, 2024. 8.

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

[9] ISO 31000:2018, Risk Management – Guidelines.

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

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

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

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

[14] NIST SP 800-171, Rev. 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, 2024. 5.

[15] NIST SP 800-30, Rev. 1, Guide for Conducting Risk Assessments, 2021. 4.

[16] NIST SP 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, 2021. 4.

[17] NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View, 2011. 3.

[18] NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations, 2020. 9.

[19] NIST SP 800-53A, Rev. 5, Assessing Security and Privacy Controls in Information Systems and Organizations, 2022. 1.

[20] NIST SP 800-53B, Rev. 5, Control Baselines for Information Systems and Organizations, 2020. 9.

[21] OWASP, Threat Modeling Process, https://owasp.org/www-community/Threat_Modeling_Process
[22] Shari Lawrence Pfleeger, “Security in Computing”, Prentice Hall, ISBN: 9780130355485, 2002. 12.
[23] The NIST Cybersecurity Framework (CSF) 2.0, NIST, 2024. 2.
[24] Threat Modeling with ATT&CK v1.0.0, https://center-for-threat-informed-defense.github.io/threat-modeling-with-attack/
[25] 공공기관의 데이터베이스 표준화 지침 (행정안전부고시 제2025-19호, 2025.2.24. 일부개정)
[26] 국가정보보안기본지침 (국가정보원, 2023.1.31. 개정)
[27] 기획재정부, 한국지능정보사회진흥원, “ISP·ISMP 수립 공통가이드”, 제8판, 2024.
[28] 사이버안보 업무규정 (국가정보원, 2024.3.5. 일부개정)
[29] 정부기능의 분류 및 관리에 관한 규정 (행정안전부, 2008.1.28. 제정)
[30] 행정안전부 정부기능별 분류체계 (공공데이터포털, 2024.12.17. 수정)
[31] 행정안전부, 한국지능정보사회진흥원, “전자정부지원사업 정보화전략계획(ISP) 산출물 점검 가이드 V1.0”, 2015.7.







1.0

국가 망 보안체계

보안 가이드라인