부록 2-11

1.0

국가 망 보안체계
보안 가이드라인

정보서비스 모델 해설서

모델 11. 정보 연계를 위한 CDS 구성

2025. 9

국가정보원

NSR 국가보안기술연구소

부록 2-11

1.0

국가 망 보안체계
보안 가이드라인

정보서비스 모델 해설서

모델 11. 정보 연계를 위한 CDS 구성

2025. 9

국가정보원

NSR 국가보안기술연구소

국가 망 보안체계
보안 가이드라인

정보서비스 모델 해설서 - 모델 11. 정보 연계를 위한 CDS 구성

부록 2-11

문서이력

개정일	버전	내역	비고
2025.1.	Draft	「국가 망 보안체계 보안 가이드라인 – 정보서비스 모델 해설서」 발간	
2025.9.	1.0	「국가 망 보안체계 보안 가이드라인 – 정보서비스 모델 해설서 – 모델 11. 정보 연계를 위한 CDS 구성」 발간	모델별 분리

CONTENTS

CONTENTS

● Table List

Figure List

제1장

정보서비스 모델 해설서 개요

제1절

정보서비스 모델 해설서 개요

1. 개요

본 해설서는 국가·공공기관에서 정보서비스[1] 구축·운영시 국가 망 보안체계(N2SF) 적용을 위한 보안 가이드라인 부록으로, 정보서비스 모델의 보안대책 수립을 위한 위협식별, 보안 요구사항 도출 및 보안통제 항목 선정 방법 제시를 목적으로 한다.

각급기관에서 구축·운영하고자 하는 정보서비스는 업무 환경 및 기관 특성에 따라 다른 형태로 구현되는 것이 일반적이지만, 다수 기관에서 생성형 AI, 외부 클라우드 서비스의 업무 활용 등 유사한 목적과 기능을 갖는 정보서비스의 구축이 이루어질 것으로 예상된다.

본 문서에서는 유사한 목적의 공통 정보서비스 모델을 도출하여 상위 수준에서 서비스 구조 및 구현 방법 등을 구체화하는데 참고할 수 있는 참조 모델을 제시한다. 각급기관에서 요구되는 정보서비스 모델을 정의하고 해당 모델에 적합한 보안대책 제시를 통해, 정보서비스 모델 구축·운용 시 필요한 보안대책 수립을 지원하고자 한다.

정보서비스 모델 해설서에서는 국가 망 보안체계 적용을 통해 변화하는 공공부문 주요 정보서비스 모델을 선정하여 보안 위협식별 및 그에 따르는 보안 요구사항 도출을 통한 보안 대책 수립에 초점을 맞추었으며, 각급기관이 해설서를 참조하여 보안대책을 적용 가능하도록 구성하였다.

1) 정보서비스는 업무정보를 이용해 특정 서비스를 제공하기 위해 하나 이상의 정보시스템으로 구성된 체계를 의미한다. 정보화 사업에서 정보시스템은 구축 및 운영의 대상이며, 정보시스템을 통해서 정보서비스를 제공하게 된다.

2. 문서 구조

본 문서는 「정보 연계를 위한 CDS 구성」 모델에 대해 설명하고 있으며, 2장은 CDS의 유형 및 구성에 대해 기술한다. 3장부터 4장까지는 Access/Transfer CDS에 대한 N2SF 단계와 활동 및 세부 내용에 대해 기술하고 있으며 5장에서는 MLS CDS 정보서비스를 소개한다.

표 1-1 정보 연계를 위한 CDS 구성과 N2SF 단계/활동의 대응 관계

절	항	N2SF 단계	N2SF 활동명	세부 내용
제3장 제2절 Access CDS 보안위협 식별	1. 정보서비스 구성요소 분석	준비 (Prepare)	[활동-1-5] 정보서비스 식별	정보서비스를 구성하는 네트워크, 정보시스템, 업무정보 등 세부구성 분석, 사용 시나리오 정의 등
	2. 모델링 및 C/S/O 평가	위협식별 (Identify)	[활동-3-1] 모델링 및 C/S/O 평가	정보서비스의 각 구성요소(네트워크, 정보시스템 등)에 대한 「위치-주체-객체」 모델링 및 C/S/O 평가
	3. 보안원칙 적용		[활동-3-2] 보안원칙 적용	「정보 생산·저장」 보안원칙 및 「정보 이동」 보안원칙 적용을 통하여 보안통제가 필요한 영역 확인
	4. 보안위협 식별		[활동-3-3] 보안위협 식별	정보서비스 구성에 기반하여 보안 위협 대상이 되는 정보시스템 및 네트워크 연계 지점, 서비스 위치를 파악하고 보안위협 요소 도출
제3장 제3절 Access CDS 보안 요구사항 및 보안대책	1. Access CDS에 대한 보안 요구사항 및 보안대책	보안대책 수립 (Select)	[활동-4-1] 보안 요구사항 도출	정보서비스 구축·운영 과정에서 필요한 Access CDS 보안 요구사항 정의 및 이를 기반으로 보안통제 항목 도출
			[활동-4-2] 보안통제 선택	
	2. Access CDS 연계에 대한 보안 요구사항 및 보안대책		-	Access CDS와 연계되는 정보시스템에 대한 보안통제 적용 필요성 기술
제4장 제2절 Transfer CDS 보안위협 식별	1. 정보서비스 구성요소 분석	준비 (Prepare)	[활동-1-5] 정보서비스 식별	정보서비스를 구성하는 네트워크, 정보시스템, 업무정보 등 세부구성 분석, 사용 시나리오 정의 등
	2. 모델링 및 C/S/O 평가	위협식별 (Identify)	[활동-3-1] 모델링 및 C/S/O 평가	정보서비스의 각 구성요소(네트워크, 정보시스템 등)에 대한 「위치-주체-객체」 모델링 및 C/S/O 평가
	3. 보안원칙 적용		[활동-3-2] 보안원칙 적용	「정보 생산·저장」 보안원칙 및 「정보 이동」 보안원칙 적용을 통하여 보안통제가 필요한 영역 확인
	4. 보안위협 식별		[활동-3-3] 보안위협 식별	정보서비스 구성에 기반하여 보안 위협 대상이 되는 정보시스템 및 네트워크 연계 지점, 서비스 위치를 파악하고 보안위협 요소 도출

절	항	N2SF 단계	N2SF 활동명	세부 내용
제4장 제3절 Transfer CDS 보안 요구사항 및 보안대책	1. Transfer CDS에 대한 보안 요구사항 및 보안대책	보안대책 수립 (Select)	[활동-4-1] 보안 요구사항 도출	정보서비스 구축·운영 과정에서 필요한 Transfer CDS 보안 요구사항 정의 및 이를 기반으로 보안통제 항목 도출
			[활동-4-2] 보안통제 선택	
	2. Transfer CDS 연계에 대한 보안 요구사항 및 보안대책		-	Transfer CDS와 연계되는 정보시스템에 대한 보안통제 적용 필요성 기술

제2절

정보서비스 모델 해설서 활용 방안

본 해설서는 각급기관이 국가 망 보안체계에 따라 획일적인 망 분리 정책에서 탈피하여 새로운 보안체계 하에서 AI·클라우드 등 신기술을 적용한 정보서비스를 도입하는 과정에서 도움이 될 수 있다.

본 문서에서 제안하는 보안통제 항목은 절대적인 기준이 아닌 검토 사항으로 기관의 특성에 맞게 유연하게 적용할 필요가 있다. 즉, 본 문서에서 제시하는 보안통제 항목을 모두 구현해야 한다거나 제시되지 않은 보안통제 항목은 구현하지 않아도 된다는 것을 의미하는 것은 아니다. 담당자는 보안통제 항목의 선택 및 구현 방안에 대해 신중히 결정하여야 하며, 특히 새로운 정보서비스 모델을 구축하거나 여러 정보서비스 모델을 동시에 구축하고자 할 경우, 제안된 보안위협 외에 다양한 보안위협을 추가로 고려하여 보안통제 항목을 폭넓게 검토하고 보안대책을 수립하는 것이 필요하다.

담당자는 각급기관이 운영하고자 하는 정보서비스 특성을 고려하여 2장의 CDS 유형을 검토한다. CDS는 Access/Transfer/MLS CDS의 유형으로 구분하여 각각 3장, 4장, 5장에서 정의하였으며, 각 장 2절과 같이 준비 단계의 일환으로 정보서비스 구성요소 등을 분석(「활동-1-5」)할 수 있다.

또한, 각 장 2절의 위협 식별 단계 중 모델링 및 C/S/O 평가(「활동-3-1」), 보안원칙 적용(「활동-3-2」) 활동에서 어떤 원칙에 위배될 수 있는지를 파악하고 보안위협 식별(「활동-3-3」) 활동에서 기관 네트워크 환경구성 및 보안통제 적용 구조 등을 고려하여 제시되어 있는 보안 위협 외에 추가 보안 위협에 대해 분석해야 한다.

각 장 3절에서 제시된 보안대책 수립 단계에서는 상기 위협을 바탕으로 보안 요구사항 도출(「활동-4-1」) 활동을 진행하게 되는데 앞서 추가로 제시된 위협 및 기관 네트워크 환경구조, 관련 규정 등을 고려하여 보안 요구사항을 최종적으로 도출한다. 보안통제 선택(「활동-4-2」) 활동에서는 필요시 기존에 제시된 보안통제 항목 외에 추가로 보안통제 항목을 선택하거나 제시된 보안통제 항목을 수정·삭제하는 등 세부사항을 조정하는 것이 가능하다.

제2장

정보 연계를 위한 CDS 구성

제1절

CDS 개요

CDS는 보안 영역 간 정보가 전달되거나 접근되는 과정에서 발생할 수 있는 보안 위협을 제어하기 위한 기술적 연계·통제 체계이다. CDS는 단순한 자료 전송 장치를 넘어, 정보 흐름의 승인, 검증, 무해화, 추적 등 다계층 보안 처리를 통합적으로 수행함으로써, 다양한 업무 목적의 정보 연계 요구를 안전하게 충족할 수 있도록 지원한다.

또한, CDS는 서로 다른 보안등급 또는 보안정책을 가진 두 개 이상의 영역에서 안전한 정보 교환을 지원하는 보안 통제시스템이다. 일반적으로 CDS는 업무망·인터넷망과 같은 보안 영역의 사이에 위치하며, 정보의 흐름에서 발생할 수 있는 보안 위협을 사전에 차단하고 허가된 정보만을 선택적으로 전달하여 보안 경계를 효과적으로 관리한다.

CDS는 단순한 네트워크 연결 장비가 아니라, 정보 단위의 검증 및 필터링 기능을 포함한 정책 기반 정보 통제시스템으로서, 주요 기능은 다음 표와 같다.

표 2-1 CDS 주요 기능

주요 기능	내용
보안 등급 영역 간 격리 유지	CDS는 서로 다른 신뢰 수준을 가진 네트워크 간 직접적인 연결을 차단하고, 중재 지점에서 통제된 흐름만 허용함으로써 도메인 간 논리적 격리 보장
정보의 정합성·무결성 검증	전송되는 정보는 내용에 대한 보안 검사를 거치며, 포맷 변환, 콘텐츠 무해화(CDR), 악성코드 탐지 등 다양한 기법을 통해 위험 요소 제거
일방향 또는 양방향 정보 흐름 제어	업무 목적에 따라 정보의 흐름은 단방향(One-Way) 또는 양방향(Two-Way)으로 설정되며, 각 방향별로 독립적인 검증 및 승인 절차 적용
기록 및 감사	CDS를 통해 전달되는 모든 정보는 감사 로그로 기록되며, 사후 분석 및 사고 대응을 위한 추적 가능한 형태로 관리

제2절

CDS 유형 및 구성

1. CDS 유형

CDS는 각급기관 내 보안 영역 연계 지점에서 정보자산의 보호와 업무 연속성의 균형을 달성하는 핵심 수단으로 작용하며, 정보 흐름의 방향성과 연계 형태에 따라 다음과 같이 세 가지 유형으로 구분된다.

가.「접근(Access) CDS」

Access CDS는 보안 영역 간 정보의 확인, 열람 등의 연계를 위해 활용되는 유형이다. 예를 들면, 업무 단말의 인터넷 자료 열람, 대민 정보서비스의 내부 업무시스템 정보 확인, 원격 접속 업무시스템 등에 사용되며, 데이터 유출 방지를 위해 읽기 전용, 세션 단절, 출력물 차단 등 보안 기능이 포함된다.

나.「전송(Transfer) CDS」

Transfer CDS는 보안 영역 간 파일, 문서, 자료 등을 단방향 또는 양방향으로 전송하기 위한 목적으로 활용되는 유형이다. 전송 대상 정보는 콘텐츠 정적분석, 포맷 검증, 무해화 및 관리자 승인 절차 등을 통해 검증되며, 보안 영역 내 정보시스템으로의 위협 유입을 사전에 차단한다.

다.「다중등급(MLS, Multi Level Security) CDS)」

MLS CDS는 하나의 시스템 또는 서비스에서 여러 보안등급의 데이터를 동시에 다루는 환경을 지원하는 유형이다. MLS 환경에서는 사용자와 시스템이 각각의 보안등급에 따라 권한을 분리하여 정보에 접근하며, 등급 간 격리 및 보안정책 기반의 접근통제를 구현한다.

표 2-2 CDS 유형별 비교

항목	Access CDS	Transfer CDS	MLS CDS
주요 목적	정보 열람 및 중계	정보 전송 및 반출/반입 통제	정보 열람·전송 지원 및 동적 정책 기반 통제
적용 시나리오	재택근무, 모바일 단말의 안전한 접근	공문서 반출/반입, 보고자료 전송 등	복합 정보서비스 환경 (열람, 전송, 검증 등)
정보 흐름	읽기 중심	쓰기 중심	읽기 · 쓰기 중심
사전 통제	없음(정보 열람만 가능)	전송 전 검증 수행	열람·전송 시 검증 수행
콘텐츠 검증	기본적인 세션 보호 중심	파일/데이터 포맷, 악성코드 검출 등 전송 콘텐츠 검증	전송·접근 콘텐츠 정밀 검증

표 2-3 CDS 유형별 활용(예)

CDS 유형	기술 예시
Access CDS	• 일방향 매체 구성: Sneakernet, One-way Cable • MILS 기반 보안 커널 또는 격리 아키텍처 • 보안 USB (읽기 전용 설정 + 파일 격리): 제한된 접근 기능을 통해 내부 자산 노출 없이 정보 확인 가능 • 스트리밍 전송: 외부 접근 요청에 대해 스트리밍 기반으로 내부 화면만 제공
Transfer CDS	• 일방향 전송: Data Diode, Dual Diode • 양방향 전송: Guards, Security Filter, 승인 기반 이관 • 자료전송 망연계 솔루션: 문서/파일을 복사·전달하며, 포맷/무해화/백신 검사 수행 등 • 스트리밍 망연계 솔루션: 서로 다른 도메인간 실시간 통신 연계 • 애플리케이션 레벨 정보흐름 통제 • 보안 USB: S→O 또는 O→S 전송 시 사용자 인증 및 검증 수행 등 • 특수 목적 게이트웨이: 문서 출력, 스크린 캡처 등 포함한 특수 목적 전송 환경 • 클립보드 전용 게이트웨이: 제한된 정보만 전송하고 나머지는 차단 (예: 텍스트만 허용)
MLS CDS	• MILS 아키텍처 기반 통합 서버: 등급별 애플리케이션/VM 격리를 유지하면서 단일 시스템에 통합 운용 • 다등급 로그 분석 시스템: 각 보안 영역의 로그를 통합 수집하되, 사용자별로 가시성 제한 • 클라우드 기반 통합 가상환경: 클라우드 시스템에서 등급별 VM/컨테이너를 분리 운영

2. CDS 구성 방법에 따른 분류

CDS는 도메인간의 안전한 정보 전달을 위해 운영하는 보안 통제시스템으로, 네 가지 구성 방법으로 구분할 수 있다. 각 구성 방법은 도메인간의 연결 방식과 CDS의 배치 위치 및 신뢰 수준에 따라 달라진다.

가.「독립형 CDS」

독립형 CDS는 신뢰되지 않는 영역(예: 인터넷)과 신뢰 영역(예: 업무망) 사이의 단일 경로상에 연결되어 존재하는 구조이다. 이 CDS는 양측 도메인과 직접 연결되며, 정보 흐름의 유일한 경로로서의 역할을 수행한다. 보안 기능과 정책 적용이 CDS 단일 지점에 집중되므로 통제가 용이하다는 장점이 있으나, CDS 자체에 대한 보안 위협 발생 시 전체 흐름이 차단될 수 있는 단일 장애점 구조를 갖는다.

나.「비신뢰형 CDS (Untrusted CDS)」

비신뢰형 CDS는 신뢰되지 않은 영역 내에 CDS가 배치되어 있으며, 신뢰 영역과의 통신을 담당한다. 이 구조는 CDS 자체가 완전한 보안 대상이 아니므로, CDS로부터 신뢰 영역에 유입되는 정보를 더욱 엄격히 검증해야 한다. 보안정책 상 최소 신뢰 수준으로 간주되며, 일반적으로 단방향 송신 전용 또는 무해화 기능 강화를 통해 보안을 확보한다.

다.「 신뢰형 CDS (Trusted CDS)」

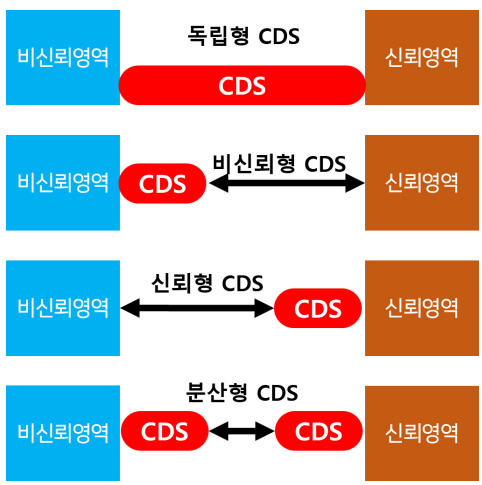
신뢰형 CDS는 신뢰 영역 내부에 CDS가 위치하는 구조이다. 신뢰되지 않는 영역으로부터 유입되는 정보를 사전에 CDS가 받아 처리하고, 내부로의 전달 여부를 판단한다. 이 경우 CDS는 비교적 높은 신뢰를 기반으로 운영되며, 내부 보안 정책과 통합되어 승인 기반의 이중 확인, 파일 변환, 정형화된 포맷 검증 등의 기능을 수행할 수 있다. 높은 보안성과 함께 정책 통합이 용이한 구조이다.

라.「분산형 CDS (Distributed CDS)」

분산형 CDS는 양쪽 도메인 각각에 CDS를 배치하고 이들이 상호 협력하여 정보 전달을 수행하는 구조이다. 일반적으로 신뢰되지 않는 영역의 CDS는 송신을 담당하고, 신뢰 영역의 CDS는 수신 및 검증을 담당한다. 이 구조는 상호 독립적인 정책 적용, 이중 방어구조, 네트워크 수준 분리 등의 장점을

가지며, 특히 상호 비대칭 신뢰 환경이나 다중 보안등급(MLS: Multi Level Security) 환경에서 효과적이다. 복잡한 정책 조정이 필요하지만, 보안성과 유연성을 동시에 확보할 수 있는 방식이다.

그림 2-1 CDS 구성 방법(예)



제3장

Access CDS

제1절

Access CDS 정의

Access CDS는 서로 다른 보안 수준을 가진 영역 간에 정보의 실시간 조회 및 열람을 안전하게 지원하는 데 특화된 유형이다. Access CDS의 핵심 목표는 높은 보안 수준 영역에 위치한 원본 데이터의 물리적 이동이나 복제를 허용하지 않고, 인가된 이용자만 필요한 정보에 접근할 수 있도록 하는 것이다. 즉, 데이터 자체는 안전한 위치에 그대로 유지한 채, 제한된 방식의 '가시성'만을 선택적으로 제공하는 접근 통제 방식이다.

또한 Access CDS는 필수적으로 프로토콜 분리 및 화면 정보 스트리밍 기술에 기반하여야 한다. 예를 들어, 내부망 사용자가 외부 인터넷 자료를 열람할 때 Access CDS는 요청을 중계하여 격리된 가상 환경에서 웹사이트에 대신 접속한다. 이후 해당 웹페이지의 화면 정보를 이미지나 비디오 스트림 형태로 변환하여 사용자 단말에 전송한다. 이로써 사용자는 실제 인터넷에 직접 연결되지 않고도 필요한 정보를 확인할 수 있으며, 외부 악성코드가 내부망으로 유입될 수 있는 네트워크 경로는 원천적으로 차단된다.

이러한 목적을 달성하기 위해 Access CDS는 다음과 같은 강력한 보안 기능을 내장한다.

표 3-1 **Access CDS 보안 기능**

보안 기능	내용
읽기 전용 강제 (Read-only)	• 사용자는 정보를 조회할 수만 있을 뿐, 수정, 편집, 삭제 등의 쓰기 작업은 원천적으로 통제되어 정보의 무결성을 보장한다.
세션 기반 연결 및 단절	• 사용자의 모든 정보 열람은 엄격히 통제된 세션 내에서만 이루어지며, 사용 종료 시 해당 세션을 완전히 소멸시켜 비인가된 접속 경로가 남지 않도록 관리한다.
데이터 유출 방지 (DLP, Data Leakage Prevention)	• 화면 캡처, 복사 및 붙여넣기(Copy & Paste), 파일 다운로드, 인쇄 등 정보가 외부로 유출될 수 있는 모든 경로를 정책에 따라 차단한다. • 필요시 화면 워터마크를 적용하여 정보 출처의 추적성을 확보한다.

결론적으로 Access CDS는 정보 접근의 편의성과 강력한 보안 통제라는 두 가지 요구사항의 균형을 맞추며, 안전한 정보 열람 환경을 구현하는 핵심 보안 연계 수단이다.

제2절

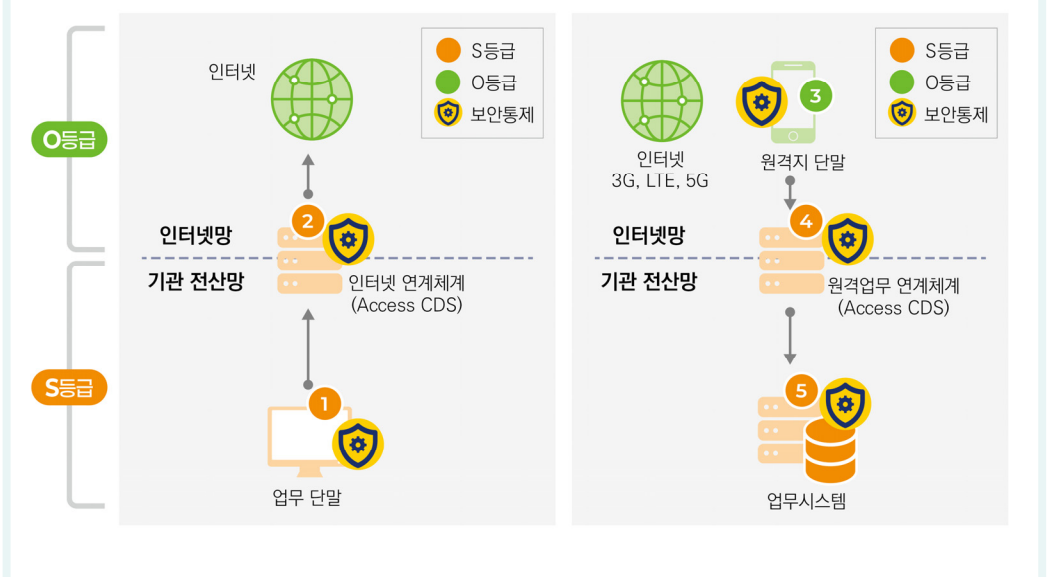
Access CDS 보안위협 식별

1. 정보서비스 구성요소 분석

본 정보서비스는 보안 영역 간 정보의 연계가 필요한 환경에서, 안전한 정보 조회, 확인, 열람 등을 위해 Access CDS를 구성하여 구축·운용하는 모델이다.

본 정보서비스는 Access CDS를 구성하는 모델의 예시이며, 업무 단말에서 인터넷 업무 수행을 위해 Access CDS를 통해 연계체계를 구성한 모델과 원격업무 수행을 위해 Access CDS를 활용하는 연계체계 구성 모델을 나타낸다. 정보서비스 모델 보안등급은 다음 그림과 같다.

그림 3-1 Access CDS 정보서비스 구성요소 분석



2. 모델링 및 C/S/O 평가

Access CDS를 포함하여 구성하는 본 정보서비스는 구성요소 분석 예시와 같이 기관 전산망 내부에서 인터넷 업무수행을 위해 연계체계에 접속하는 모델과 기관 외부 원격지 단말에서 원격업무 수행을 위해 연계체계에 접속하는 모델로 구분할 수 있다. 따라서 모델링 및 C/S/O 평가를 각 모델별로 구분하여 평가한다.

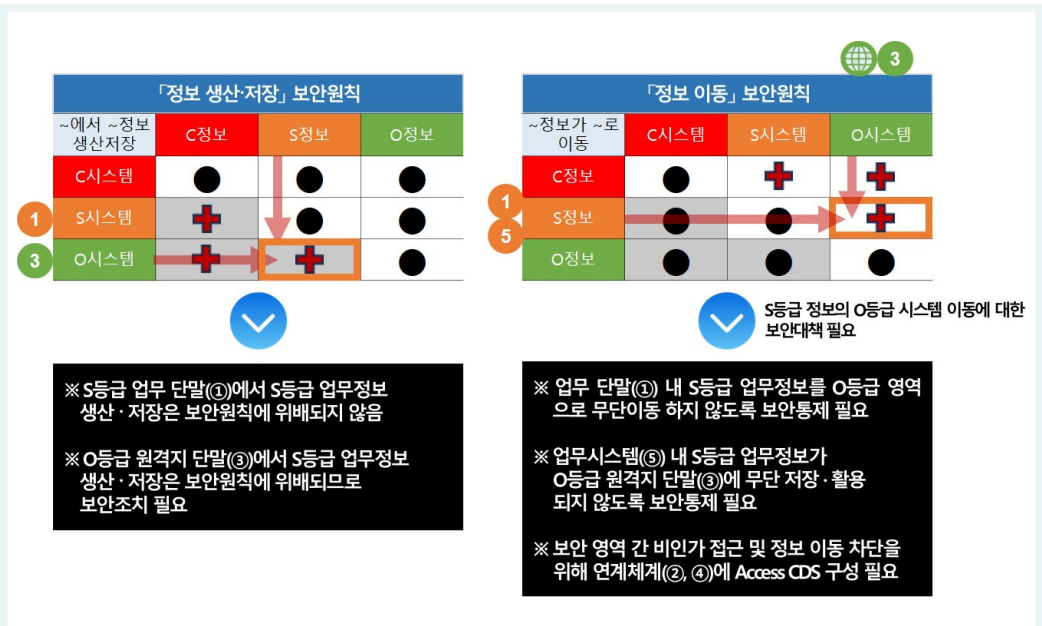
첫째, 업무 단말의 인터넷 활용 모델에서는 「위치(기관 청사)-주체(이용자 단말)-객체(인터넷 서비스)」로 모델링 할 수 있고, 이때 보안등급은 위치 S등급, 주체 S등급 및 객체 O등급으로 평가한다.

둘째, 기관 외부의 원격지 단말이 연계체계를 경유하여 기관 전산망 내 업무시스템에 접속하는 모델에서는 「위치(인터넷)-주체(원격지 단말)-객체(업무시스템)」로 모델링 할 수 있고, 이때 보안등급은 위치 O등급, 주체 O등급 및 객체 S등급으로 평가한다.

그림 3-2 Access CDS 「위치-주체-객체」 모델링 및 C/S/O 평가

3. 보안원칙 적용

그림 3-3 Access CDS 보안원칙 적용



가. 「정보 생산·저장」 보안원칙 적용

첫 번째 예시에서 기관 전산망에 위치한 업무 단말은 S등급이며, S등급 및 O등급 업무정보 취급은 「정보 생산·저장」 보안원칙에 위배되지 않는다.

두 번째 예시에서 인터넷 영역에 위치한 원격지 단말은 O등급이며, S등급 업무정보 취급은 「정보 생산·저장」 보안원칙에 위배되기에 보안통제 적용이 필요하다.

나. 「정보 이동」 보안원칙 적용

첫 번째 예시에서 기관 전산망에 위치한 업무 단말은 S등급이며, 인터넷 서비스는 O등급이다. 따라서 업무 단말 내 S등급 정보가 인터넷 서비스에 무단 이동되지 않도록 보안통제가 필요하다.

두 번째 예시에서 인터넷과 연결된 원격지 단말은 O등급이며, 업무시스템을 통해 조회하는 업무정보는 S등급이다. 따라서 업무시스템 내 S등급 정보가 원격지 단말에 무단 이동되지 않도록 보안통제가 필요하다.

본 정보서비스 모델 예시에서는 S등급 기관 전산망과 O등급 영역 간 비인가 접근 및 무단 정보 이동 등을 차단하기 위해 연계체계에서 보안통제가 필요하다고 판단하였다. 따라서, 연계체계 내 Access CDS를 구성하여 외부 영역으로부터의 기관 전산망 비인가 접근 차단 및 업무 정보의 무단 이동을 방지한다.

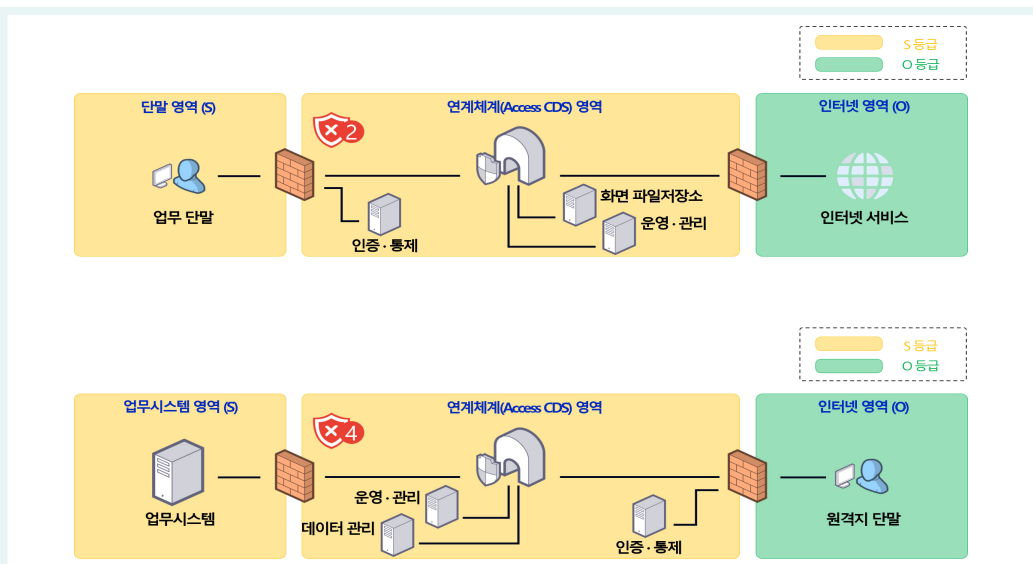
또한, 외부 단말에서 원격으로 열람 중인 화면에 대해 캡처, 복사, 인쇄 등 기능을 통해 정보가 외부로 유출되지 않도록 해당 기능 차단 등 보안통제를 적용해야 하며, Access CDS를 통해 전송되는 정보의 등급 변환이 이루어지는 경우 기관 정책에 따른 사전 검토·승인 절차 적용을 검토해야 한다.

Access CDS를 구성하는 본 정보서비스 모델은 예시이며, 기관 업무환경과 정보서비스 구축 시 업무 특성을 고려하여 Access CDS 구성 및 보안원칙 적용 과정을 수행해야 한다.

4. 보안위협 식별

Access CDS를 구성하는 정보서비스 예시는 업무 단말에서 인터넷 서비스를 활용하기 위한 모델과 원격업무를 위해 원격지 단말을 통한 업무시스템 접속 모델로 구분하였으며, 〈표 3-2〉와 같이 정보서비스 모델 구성 중 연계체계(Access CDS)를 대상으로 보안 위협을 식별한다.

그림 3-4 Access CDS 보안위협 대상 식별



Access CDS를 구성하는 본 정보서비스 모델은 예시이며, 기관 업무환경 및 정보서비스 특성을 고려하여 Access CDS 구축·운영 시 환경구성 및 보안위협 대상을 식별해야 한다.

표 3-2 Access CDS 보안 위협

대상	구분	보안위협 번호	보안위협 요소
연계 체계	②, ④ Access CDS	TH-M11-1	연계체계 비인가 접근
		TH-M11-2	이용자 인증 우회
		TH-M11-3	비인가 정보 접근 및 유출
		TH-M11-4	비인가 보안 영역 접근
		TH-M11-5	보안 영역 간 비인가 네트워크 연결
		TH-M11-6	연계체계 인증 정보 유출
		TH-M11-7	관리자 기능 비인가 접근
		TH-M11-8	비인가 매체 연결 및 기능 실행
		TH-M11-9	취약점 노출 및 악용
		TH-M11-10	정보 접근 이력 변조

제3절

Access CDS 보안 요구사항 및 보안대책

기관은 국가 망 보안체계(N2SF) 정보서비스 모델의 안전한 활용을 위해 「정보 생산·저장」 및 「정보 이동」 보안원칙을 준수해야 하며, Access CDS를 구성한 정보서비스 구축·운영 시 연계 지점에서 보안위협을 식별하고 이에 대한 보안대책을 적용해야 한다.

정보서비스 구성요소 분석, 모델링 및 C/S/O 평가, 보안원칙 적용, 보안위협 식별 과정을 통해 위협을 파악하고, 정보서비스 모델 보안대책 수립 방향성과 국가·공공기관의 정책적 요구사항을 반영하여 보안 요구사항 및 N2SF 보안통제 항목을 선정하였다.

표 3-3 Access CDS 보안 요구사항 및 보안통제 항목

구분(유형)	구성요소	보안위협	보안 요구사항	N2SF 보안통제 항목
연계 체계	②, ④ Access CDS	(TH-M11-1) 연계체계 비인가 접근 (TH-M11-2) 이용자 인증 우회	Access CDS 비인가 접근 차단	N2SF-AC-1 N2SF-AC-1(1) N2SF-AC-1(2) N2SF-AC-1(3) N2SF-AC-1(4) N2SF-AC-3 N2SF-DA-3 N2SF-DA-4 N2SF-LI-1 N2SF-LI-2 N2SF-LI-4
		(TH-M11-3) 비인가 정보 접근 및 유출	Access CDS 데이터 접근 제어	N2SF-CD-1 N2SF-CD-4 N2SF-CD-8 N2SF-CD-10 N2SF-CD-12 N2SF-CD-M1 N2SF-CD-M2 N2SF-CD-M3 N2SF-CD-M4

구분(유형)	구성요소	보안위협	보안 요구사항	N2SF 보안통제 항목
		(TH-M11-4) 비인가 보안 영역 접근 (TH-M11-5) 보안 영역 간 비인가 네트워크 연결	Access CDS 네트워크 제어	N2SF-IS-4 N2SF-IF-1 N2SF-IF-6 N2SF-IF-9 N2SF-EB-3
		(TH-M11-6) 연계체계 인증 정보 유출	Access CDS 인증 정보 보호	N2SF-AU-5 N2SF-AU-5(1) N2SF-AU-5(2) N2SF-AU-M1
		(TH-M11-7) 관리자 기능 비인가 접근 (TH-M11-8) 비인가 매체 연결 및 기능 실행	Access CDS 보안성 유지	N2SF-LP-1 N2SF-LP-4 N2SF-LP-4(1) N2SF-LP-4(4) N2SF-AC-1(5) N2SF-AC-3(1) N2SF-EB-8 N2SF-EB-10 N2SF-EB-11 N2SF-EB-13 N2SF-DV-4 N2SF-DV-6 N2SF-DV-10 N2SF-DV-12 N2SF-IN-1(1) N2SF-IN-5 N2SF-IN-6 N2SF-IN-11
		(TH-M11-9) 취약점 노출 및 악용 (TH-M11-10) 정보 접근 이력 변조	Access CDS 운용 관리	N2SF-LP-M1 N2SF-LP-M2 N2SF-AC-1(2) N2SF-AC-M1 N2SF-AC-M2 N2SF-AC-M3 N2SF-LI-M1 N2SF-LI-M2 N2SF-IS-2 N2SF-IF-M1 N2SF-IF-M2 N2SF-IF-M3 N2SF-IF-M4 N2SF-IF-M5 N2SF-EB-M5

1. Access CDS에 대한 보안요구사항 및 보안대책

Access CDS는 보안 영역 간 정보 접근이 필요한 경우에 안전한 접근을 중계·통제하는 핵심 보안 구성요소이다. Access CDS를 포함하는 정보서비스 모델에서는 Access CDS 접속 시부터 연결 종료 시까지 보안통제가 적용되어야 한다. 본 해설서에서는 Access CDS를 대상으로 보안 요구사항 및 보안대책을 기술하며, 기관 환경 및 운영하고자 하는 정보서비스 특성을 고려하여 보안대책 수립을 검토해야 한다.

Access CDS가 구성된 정보서비스 구축·운영 시 다음과 같은 보안 요구사항 및 보안통제 항목을 적용해야 한다.

① 「Access CDS」 비인가 접근 차단

Access CDS는 사전 승인된 사용자 및 등록된 단말·시스템만 접근할 수 있도록 구성되어야 하며, 비인가된 단말·시스템이나 변조된 애플리케이션을 통한 접근은 인증 단계에서 차단해야 한다. 인증되지 않은 접근은 세션 생성 이전에 탐지 및 차단되어야 한다.

② 「Access CDS」 데이터 접근 제어

Access CDS를 통한 데이터 흐름은 업무 등급(S·O 등급) 간의 구간을 넘나들므로, 데이터 열람 시 메타데이터 및 데이터 본문의 불필요한 확산을 막고, 열람 종료 시 모든 캐시·임시 데이터는 자동 삭제되어야 한다. 동시에, 접근한 정보에 대해 다운로드, 복사, 인쇄, 화면 캡처 등은 통제되어야 하며, 정보 흐름은 로깅되어야 한다.

Access CDS는 인증 후, 업무 역할 및 유형에 따라 접근 가능한 데이터 등급(S등급, O등급)을 분리·통제해야 한다. 필요 최소한의 접근 권한만을 부여하며, 인증된 단말·시스템이라도 허가받지 않은 상위 보안등급 정보는 접근이 제한되어야 한다.

③ 「Access CDS」 네트워크 제어

Access CDS 인증 우회 시도 및 사전 승인된 기관 전산망 외 비인가 네트워크로의 접근을 차단해야 한다.

Access CDS를 통해 보안 영역 간의 통신을 연계해야 하며, 직접적인 네트워크 연결은 물리적·논리적으로 차단 등 보안대책을 적용해야 한다. Access CDS가 요청 및 응답을 중계·검증함으로써 상호 신뢰 수준을 조정하는 통제점이 되어야 한다.

비인가 네트워크 프로토콜은 차단해야 한다.

Access CDS는 연결 세션의 생성·유지·종료를 실시간으로 통제하며, 일정 시간 이상 비활동 시 자동 연결 종료 처리되어야 한다. 생성된 세션의 모든 요청·응답 흐름은 감사 로그로 저장되며, 해당 로그는 위·변조되지 않도록 안전하게 보관되어야 한다.

④ 「Access CDS」 인증 정보 보호

Access CDS 이용자 및 단말·시스템 인증 정보 변경에 대한 관리 정책을 수립하여, 무단 변경 등을 방지해야 한다.

Access CDS 인증 정보가 유출되지 않도록 정보 관리 정책을 수립해야 하며, 인증 정보 유출 시 대응 절차를 마련해야 한다.

⑤ 「Access CDS」 보안성 유지

Access CDS 관리자 권한 계정을 일반 사용자 계정과 분리하여 관리해야 하며, 비인가 장치의 연결 등을 통제해야 한다.

Access CDS의 취약점으로 인해 보안위협이 발생하지 않도록 최신 보안 업데이트 등 보안성을 유지해야 한다.

Access CDS에 비인가 기능·소프트웨어의 설치·실행 및 비인가 형상 변경으로 인한 보안위협이 발생하지 않도록 형상관리 등을 수행해야 한다.

그 외 기관 업무환경에 필요한 Access CDS의 보안 조치가 완료되어야 한다.

⑥ 「Access CDS」 운용 관리

Access CDS의 관리자 기능은 최소 권한 사용자만 접근 가능해야 하며, 관리자 작업 이력(로그인 시각, 설정 변경, 정책 적용 등)은 모두 기록되어야 한다. 설정 변경, 사용자 등록, 시스템 업데이트 등 주요 기능 실행에 대한 2인 승인 및 검토 절차가 마련되어야 한다.

Access CDS의 모든 접근 및 흐름 기록은 정보보안담당자가 주기적으로 확인할 수 있도록 로그로 저장되고, 로그 접근 권한은 분리되어야 하며, 삭제·변경은 시스템적으로 제한되어야 한다.

기관은 위와 같은 보안 요구사항 및 〈표 3-4〉의 보안통제 항목을 포함하는 보안대책을 준수해야 한다.

표 3-4 Access CDS 보안통제 항목

코드	보안통제 항목	내용
① Access CDS 비인가 접근 차단		
N2SF-AC-1	계정 관리 자동화	• 정보시스템 계정 관리를 효율화하고, 인적 오류를 최소화하기 위해 자동화된 메커니즘을 사용하여 계정 관리를 수행한다.
N2SF-AC-1(1)	동적 계정 관리	• 사용자 상태(입사, 퇴사, 부서 이동 등)에 따라 계정 정보를 실시간으로 반영하고, 시스템 간 계정 동기화를 통해 계정 수명주기 관리를 자동화한다.
N2SF-AC-1(2)	계정 상태 모니터링	• 계정의 임시 생성, 수정, 활성화, 비활성화 및 삭제 등을 모니터링한다.
N2SF-AC-1(3)	계정 자동 비활성화	• 계정 사용 기간이 종료되거나 일정 기간 미사용된 계정은 자동으로 비활성화한다.
N2SF-AC-1(4)	계정 자동 로그아웃	• 비활동 시간이 일정 기간 지속되었을 때 정보시스템에서 자동 로그아웃 되어야 한다.
N2SF-AC-3	의심스러운 계정 모니터링	• 비정상적이거나 의심스러운 계정 접속 시도 및 활동을 지속적으로 모니터링한다.
N2SF-DA-3	단말 식별 및 인증	• 단말의 고유 식별자(MAC, TPM, 인증서 등)를 통해 단말을 식별하고, 등록된 단말만 인증을 통해 시스템에 접근할 수 있도록 한다.
N2SF-DA-4	인증된 단말의 접속 관리	• 인증된 단말이라 하더라도 접속 시간, 위치, 사용자에 따라 세부 접근 권한을 제어하고, 접근 이력을 기록하여 감사 가능하도록 한다.
N2SF-LI-1	유효한 인증정보 노출 방지	• 인증 과정에서 유효한 인증 정보가 노출되지 않도록 한다.
N2SF-LI-2	로그인 실패에 따른 접속 제한	• 정의한 횟수 이상 연속적으로 로그인을 실패한 경우 일정시간 계정을 차단(또는 잠김)하거나 접속을 제한한다.
N2SF-LI-4	계정 잠금 해제 인증요소 추가	• 계정 잠금 상태에서 해제 요청 시 기본 인증 요소 외 인증요소를 추가 사용한다.
② Access CDS 데이터 접근 제어		
N2SF-CD-1	도메인 간 정보 흐름 검증 및 통제	• 서로 다른 보안 도메인 간 정보 흐름 시 데이터 유형, 등급, 출처를 검증하고 사전에 정의된 정책에 따라 전송을 허용, 차단 또는 보류한다.
N2SF-CD-4	검증 기반 릴레이 시스템 적용	• 수신된 정보는 릴레이 서버를 통해 악성코드 스캔, 포맷 검증, 콘텐츠 정제 후 안전성 판단을 거쳐 송신된다.
N2SF-CD-8	승인된 CDS 구성요소만 사용	• 크로스 도메인 연계를 위한 CDS는 기관이 검증하고 승인한 하드웨어/소프트웨어 구성요소만을 사용해야 한다.
N2SF-CD-10	전송 실패 보호 및 무결성 보장	• 전송 중 실패 시 데이터가 잔존하거나 일부가 누락되지 않도록 조치하고, 수신자가 정보의 완전성과 무결성을 검증할 수 있도록 한다.
N2SF-CD-12	사용자 및 단말 등록 기반 접근 제어	• CDS 접근을 허용할 사용자와 단말 정보를 사전에 등록하고, 정책에 기반해 인증을 수행한다.
N2SF-CD-M1	CDS 운용 정책 수립	• CDS 구성, 운용, 접근, 예외 처리 절차 등을 포함한 관리 정책을 수립하고 주기적으로 갱신한다.

코드	보안통제 항목	내용
N2SF-CD-M2	CDS 통제 로그 기록 및 감사	• CDS를 통한 정보 흐름의 허용, 차단, 예외처리 등의 모든 활동을 로깅하고 주기적으로 감사한다.
N2SF-CD-M3	도메인 간 정보 교환 승인 프로세스	• 도메인 간 정보 교환은 사전 승인된 업무 목적 및 사용자에 한정되며, 자동화된 승인 및 검토 체계를 갖추어야 한다.
N2SF-CD-M4	CDS 구성요소 무결성 검증	• CDS 시스템의 구성요소(소프트웨어, 펌웨어 등)에 대한 무결성을 정기적으로 검증하고 변경 시 승인 절차를 거친다.
③ Access CDS 네트워크 제어		
N2SF-IS-4	네트워크 격리	• 내부망, 외부망, 보안망 등 네트워크 간에 방화벽, 라우팅 제어 등으로 트래픽을 분리하여 정보 유출 또는 확산을 방지한다.
N2SF-IF-1	정보흐름의 동적 통제	• 정보시스템의 비정상 동작, 외부의 공격 등 지정한 조건에 대하여 정보흐름을 동적으로 통제한다.
N2SF-IF-6	필터링 규칙 정보흐름 통제	• 보안 및 프라이버시 등에 관한 필터링 규칙을 적용하여 정보흐름을 통제한다.
N2SF-IF-9	출발지점과 도착지점 식별 및 인증	• 정보 전송 시 개인, 기관, 응용프로그램 혹은 정보시스템 등 하나 이상을 사용하여 출발지점과 도착지점을 식별하고 인증한다.
N2SF-EB-3	화이트리스트 기반 통신 허용	• 기본적으로 모든 통신을 차단한 상태에서 필요한 통신만을 허용하는 화이트리스트 기반 정책을 적용한다.
④ Access CDS 인증 정보 보호		
N2SF-AU-5	인증 시스템 구성 및 관리	• 인증 시스템의 구성 요소를 안전하게 설정하고 변경 시 보안에 영향이 없도록 관리한다.
N2SF-AU-5(1)	비밀번호 보안수준 점검	• 자동화된 도구를 이용하여 비밀번호 정책에 적합하게 설정·유지되고 있는지 점검한다.
N2SF-AU-5(2)	대체 보안수단 강구	• 보안 기능을 구현 또는 제공하는 주요 수단을 사용할 수 없거나 손상되었을 상황을 대비한 대체 보안수단을 강구한다.
N2SF-AU-M1	인증 정보 접근 권한 통제 및 관리	• 인증 정보는 최소한의 인원만 접근할 수 있도록 제한하고 기록을 남긴다.
⑤ Access CDS 보안성 유지		
N2SF-LP-1	정보시스템 접근 권한 정의	• 업무정보(데이터)를 식별하고, 업무정보를 저장하고 있는 정보시스템 접근 권한을 정의한다.
N2SF-LP-4	관리자 권한 제한	• 정보시스템 접근에 필요한 최소한의 관리자 및 운영자 등에게만 관리자 권한을 부여한다.
N2SF-LP-4(1)	원격접속을 통한 관리자 권한 접속제한	• 기관 네트워크 내부에서 관리자 권한 접속이 제한되는 경우 등 불가피한 상황에서만 한시적으로 기관 네트워크 외부에서의 관리자 권한 접속을 허용하며, 목적이 달성된 경우 외부에서의 관리자 권한 접속을 즉시 차단한다.
N2SF-LP-4(4)	관리자 권한 실행 로깅 및 감사	• 관리자 권한 기능 실행 내역은 로깅하고 주기적인 사용 내역 감사를 실시한다.

코드	보안통제 항목	내용
N2SF-AC-1(5)	불필요한 관리자 권한 계정 제거	• 관리자 권한이 필요 없거나 활용이 종료된 계정은 비활성화 또는 삭제 조치한다.
N2SF-AC-3(1)	위험에 노출된 계정 비활성화	• 정보시스템 위협 탐지 시, 위협에 노출된 계정은 신속히 비활성화하거나 제한 조치를 한다.
N2SF-EB-8	운영관리용 포트의 물리적 연결 차단	• 운영관리용 포트에 인가되지 않은 장치의 포트 연결을 차단한다.
N2SF-EB-10	정보시스템 구성요소 외부 노출 차단	• 정보시스템 운영관리 및 서비스를 제공하는 구성요소가 외부 노출되지 않도록 차단한다.
N2SF-EB-11	외부 경계 보호 기능 유지	• 외부 경계를 보호하는 정보자산(보안시스템 등) 장애 시에도 보호기능은 유지되도록 구성한다.
N2SF-EB-13	오류정보 발신자 전송 제한	• 네트워크 규약에 따른 통신 오류 발생 시 발신자에게 피드백이나 경고를 통해 정보시스템 구성이나 취약점이 전송되지 않도록 한다.
N2SF-DV-4	포트 및 입출력 장치 제어	• 정보시스템의 포트나 입출력 장치를 제어하여 악성코드 유입 및 정보 유출을 차단한다.
N2SF-DV-6	통신 기능이 포함된 저장장치 제한	• 통신기능이 포함된 저장장치를 사용을 제한한다.
N2SF-DV-10	저장장치 연결 금지	• 정보시스템 기동 및 종료 또는 재시작하는 동안 쓰기 가능한 저장장치 연결을 금지한다.
N2SF-DV-12	장치 펌웨어 업데이트 검증	• 펌웨어 업데이트 시 서명 검증 또는 위변조 여부를 검증하여 설치를 제한한다.
N2SF-IN-1(1)	정보시스템 구성요소 최신상태 유지	• 정보시스템 내의 모든 구성요소가 포함되도록 정보시스템 구성 요소 목록을 작성하고 정기적으로 검토 및 최신 상태로 업데이트 한다.
N2SF-IN-5	비인가 변경 방지	• 인가되지 않은 정보시스템 구성요소 변경을 방지한다.
N2SF-IN-6	불필요한 구성요소 제거	• 필요 기능만 제공하도록 구성하고, 사용하지 않는 기능, 포트, 프로토콜, 소프트웨어, 서비스의 사용을 제거하거나 비활성화한다.
N2SF-IN-11	재기동 서비스 신뢰성 확보	• 정보시스템 구성요소와 서비스가 재기동(재부팅) 할 때 소프트웨어와 데이터는 신뢰된 곳으로부터 획득한다.
⑥ Access CDS 운용 관리		
N2SF-LP-M1	특별권한 사용자 지정	• 일반 사용 권한과 별도로 특별권한 사용자 그룹을 지정하고, 이들의 권한 부여와 변경을 통제한다.
N2SF-LP-M2	주요 사용자 위험 관리	• 주요 사용자의 권한과 활동을 모니터링하고 이상 징후를 탐지하여 위험을 사전에 관리한다.
N2SF-AC-1(2)	계정 상태 모니터링	• 계정의 임시 생성, 수정, 활성화, 비활성화 및 삭제 등을 모니터링한다.
N2SF-AC-M1	감사 활동 자동화	• 계정 사용 및 관련된 감사 활동을 자동화하여 관리

코드	보안통제 항목	내용
N2SF-AC-M2	감사기록 생성	• 계정 활동에 대한 감사 기록을 생성하여 보관 및 분석할 수 있도록 함
N2SF-AC-M3	세션 감사	• 세션 활동을 기록하고 주기적으로 감사하여 비정상적 행위 탐지
N2SF-LI-M1	로그인 실패 모니터링 및 보고	• 반복 실패, 의심 로그인 시도 등의 실패 패턴을 실시간 감지하고 관리자에게 보고
N2SF-LI-M2	주기적 로그인 정보 무결성 점검	• 로그인 관련 데이터(세션, 토큰, 사용자 매핑 정보 등)에 대해 주기적인 무결성 점검 및 이상 여부 확인
N2SF-IS-2	정보시스템 운영·관리 기능 표출 제한	• 일반 사용자에게 정보시스템 관리와 관련된 기능 및 인터페이스 표출을 제한한다.
N2SF-IF-M1	정보흐름 통제 정책 수립 및 갱신	• 정보 흐름에 대한 통제 기준 및 예외 절차를 문서화하고 정기적으로 갱신한다.
N2SF-IF-M2	정보흐름 로그 기록 및 보존	• 정보 흐름 통제 활동(허용/차단 등)을 로깅하고, 법적/감사 목적으로 일정 기간 보관한다.
N2SF-IF-M3	정보흐름 통제 감사 및 이행 점검	• 정보 흐름 통제의 적용 현황을 정기적으로 점검하여 정책 미준수 사항 식별 및 개선
N2SF-IF-M4	비인가 흐름 탐지 자동화	• 정책을 우회하거나 비정상적 흐름을 탐지하기 위한 자동화 도구 또는 시스템 구축
N2SF-IF-M5	통제 실패·예외 보고 체계	• 통제가 실패하거나 예외 발생 시 담당자에게 자동 보고하고 이를 기록하는 체계를 마련한다.
N2SF-EB-M5	비상 시 외부 통신 격리	• 침해 발생 시 외부 통신을 즉시 차단할 수 있는 절차를 마련한다.

2. Access CDS 연계에 대한 보안 요구사항 및 보안대책

Access CDS를 구성한 정보서비스 모델에서는 Access CDS과 연계하는 보안 영역의 단말, 시스템 등에 대한 보안대책 적용이 필요하다. 본 해설서에서 기술한 정보서비스 모델은 예시이며, 기관이 구축·운영하고자 하는 정보서비스의 업무 목적 및 특성을 고려하여 단말·시스템의 보안성 유지, 인증, 운영 관리, 네트워크 통제 등 보안 요구사항 및 보안통제 항목을 적용해야 한다.

제4장

Transfer CDS

제1절

Transfer CDS 정의

Transfer CDS는 보안 정책에 따라 두 보안 영역 간에 파일이나 정형화된 데이터의 안전한 전송을 목적으로 설계된 유형이다. Transfer CDS의 핵심 목표는 전송되는 정보 콘텐츠 자체에 잠재된 악성 코드나 위협 요소를 제거하고, 오직 승인된 형식과 내용의 데이터만이 경계를 통과하도록 보장하여 내부 정보 시스템의 안정성과 신뢰성을 확보하는 것이다.

Transfer CDS는 필수적으로 서로 다른 보안영역간 데이터 전송시 통신이 직접 연결되지 않고 내부적으로 전송 프로토콜을 분리하면서 컨텐츠에 대한 보안통제를 적용하는 기술에 기반하여야 한다.

전송 과정은 단방향 또는 양방향으로 구성될 수 있으며, 다음과 같은 절차를 거친다.

표 4-1 Transfer CDS 보안 절차

보안 절차	내용
임시 격리 및 분석	• 전송 요청된 파일은 목적지로 즉시 전달되지 않고, Transfer CDS 내부에 마련된 격리 저장소에서 정밀 분석을 수행한다.
콘텐츠 정적 분석 및 포맷 검증	• 파일의 구조와 내용을 분석하여 알려진 악성코드 패턴이나 비정상적인 스크립트 유무를 탐지한다. • 파일의 확장자와 실제 데이터 형식이 일치하는지 검증하여 위장된 실행 파일 등의 위협을 차단한다.
무해화 (Sanitization/CDR)	• 문서 파일 내부에 포함될 수 있는 매크로, 스크립트 등 잠재적 위협이 될 수 있는 동적 콘텐츠를 원천적으로 제거하고, 순수한 데이터만으로 파일을 재구성한다. ※ 알려지지 않은 신종 위협 대응을 위한 수단으로 활용 가능
관리자 승인	• 중요 자료의 경우, 자동화된 검증 절차 완료 후에도 보안 관리자의 최종적인 검토 및 승인을 거쳐야만 전송이 완료되도록 워크플로우를 구성하여 통제 절차를 보완할 수 있다.

이처럼 Transfer CDS는 외부로부터의 패치 파일이나 업무 자료를 내부망으로 안전하게 반입하거나, 내부 데이터를 외부로 전송하는 등 데이터의 물리적 이동이 반드시 필요한 업무에서 정보 자산의 보호와 업무 연속성을 동시에 달성하는 핵심 보안통제 수단으로 활용된다.

제2절

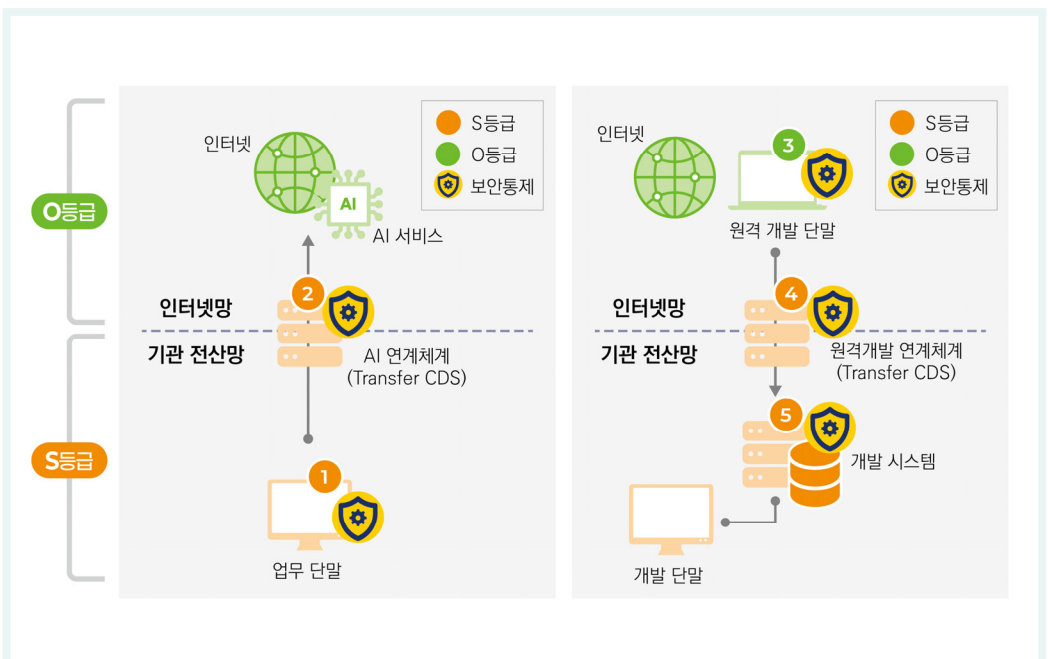
Transfer CDS 보안위협 식별

1. 정보서비스 구성요소 분석

본 정보서비스는 보안 영역 간 정보의 연계가 필요한 환경에서, 안전한 정보 전달, 업무환경 구성 등을 위해 Transfer CDS를 구성하여 구축·운용하는 모델이다.

본 정보서비스는 Transfer CDS를 구성하는 모델의 예시이며, 업무 단말에서 생성형 AI 서비스 활용을 위해 AI 연계체계를 구성한 모델과 원격지에서 원격 개발 단말을 통해 기관 전산망 개발 시스템 접속을 위한 원격개발 연계체계 구성 모델을 나타낸다. 정보서비스 모델의 보안등급은 다음 그림과 같다.

그림 4-1 Transfer CDS 정보서비스 구성요소 분석



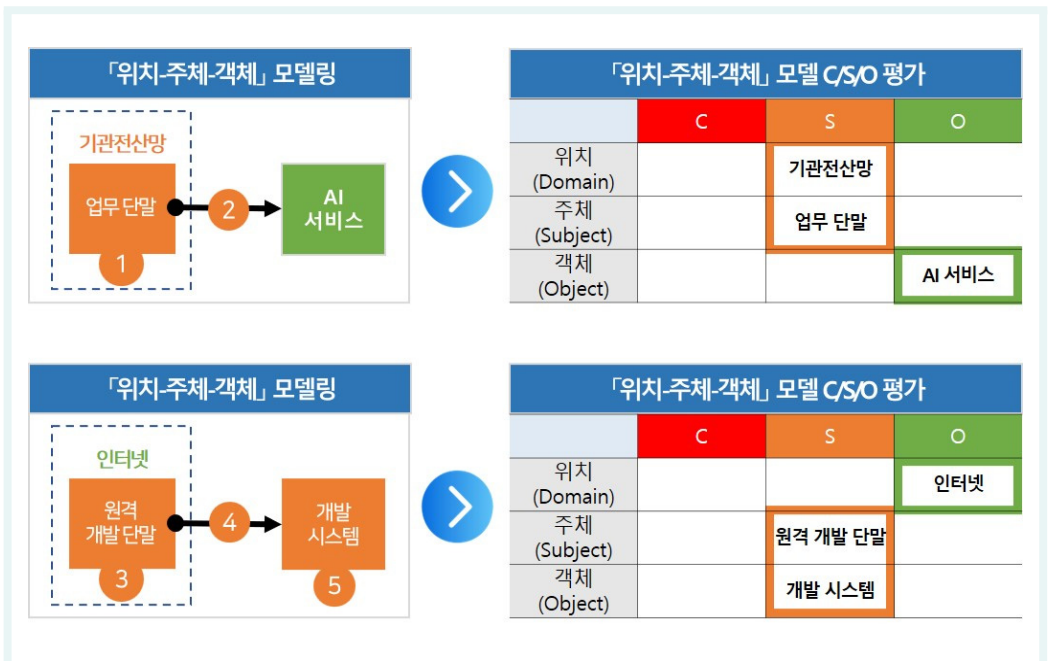
2. 모델링 및 C/S/O 평가

Transfer CDS를 포함하여 구성하는 본 정보서비스는 구성요소 분석 예시와 같이 기관 전산망 내부에서 생성형 AI 활용을 위해 연계체계에 접속하는 모델과, 원격지에서 원격 개발 단말을 통해 기관 전산망 개발 시스템에 접속하는 모델로 구분할 수 있다. 따라서 모델링 및 C/S/O 평가를 각 모델별로 구분하여 평가한다.

첫째, 업무 단말의 생성형 AI 활용 모델에서는 「위치(기관 청사)-주체(이용자 단말)-객체(AI 서비스)」로 모델링 할 수 있고, 이때 보안등급은 위치 S등급, 주체 S등급 및 객체 O등급으로 평가한다.

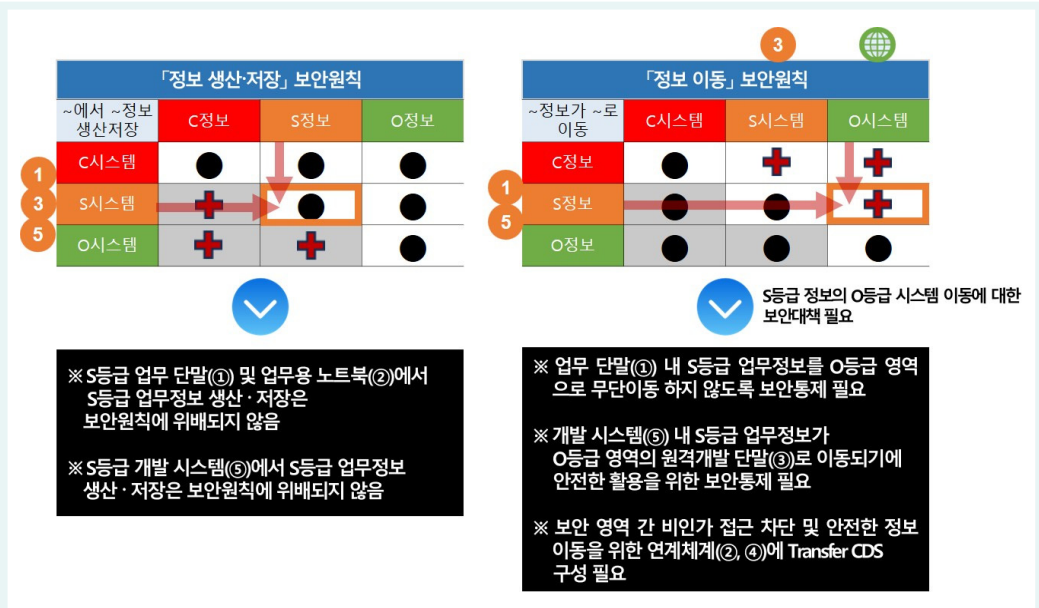
둘째, 원격지의 원격 개발 단말이 연계체계를 경유하여 기관 전산망 내 개발 시스템에 접속하는 모델에서는 「위치(인터넷)-주체(원격 개발 단말)-객체(화상화의 시스템)」로 모델링 할 수 있고, 이때 보안등급은 위치 O등급, 주체 S등급 및 객체 S등급으로 평가한다.

그림 4-2 Transfer CDS「위치-주체-객체」모델링 및 C/S/O 평가



3. 보안원칙 적용

그림 4-3 Transfer CDS 보안원칙 적용



가.「정보 생산·저장」 보안원칙 적용

첫 번째 예시에서 기관 전산망에 위치한 업무 단말은 S등급이며, S등급 및 O등급 업무정보 취급은 「정보 생산·저장」 보안원칙에 위배되지 않는다.

두 번째 예시 역시 인터넷에 위치한 원격 개발 단말은 S등급이며, S등급 및 O등급 업무정보 취급은 「정보 생산·저장」 보안원칙에 위배되지 않는다.

나.「정보 이동」 보안원칙 적용

첫 번째 예시에서 기관 전산망에 위치한 업무 단말은 S등급이며, 생성형 AI 서비스는 O등급이다. 따라서 업무 단말 내 S등급 정보가 AI 서비스에 무단 이동되지 않도록 보안통제가 필요하다.

두 번째 예시에서 인터넷 영역에 위치한 원격 개발 단말과 개발 시스템을 통해 전달되는 정보는 S등급이다. 하지만 원격 개발 단말의 위치가 O등급이기에 원격 개발 단말에서 활용되는 정보를 안전하게 관리하기 위한 보안통제가 필요하다.

본 정보서비스 모델 예시에서는 S등급 기관 전산망과 O등급 영역 간 비인가 접근 및 S등급 정보 유출 등을 차단하기 위해 연계체계에 대한 보안통제가 필요하다. 본 정보서비스 모델 예시에서는 Transfer CDS를 구성하여 외부 영역으로부터의 기관 전산망 비인가 접근 차단 및 업무 정보 유출을 방지한다.

기관 전산망에서 인터넷 등 외부 보안 영역으로 전송하는 대상 정보는 보안등급 확인, 전송 승인, 보안 검사(DLP, AV, 포맷 제한 등)를 거쳐야 하며, 전송 메타데이터(해시값, 수신자, 시점 등)를 함께 저장한다. 정보는 사전 정의된 포맷, 경로, 대상자에 한해 전송되며, 비식별화, 마스킹, 불필요 항목 제거 등 정보 축소 등을 통해 외부로 유출되는 정보를 최소화한다. 정보 유출 방지를 위해 업무 단말은 복사 방지, 캡처 차단, 출력 제한, 외부 매체 연결 차단 등의 보안정책을 준수하여야 한다.

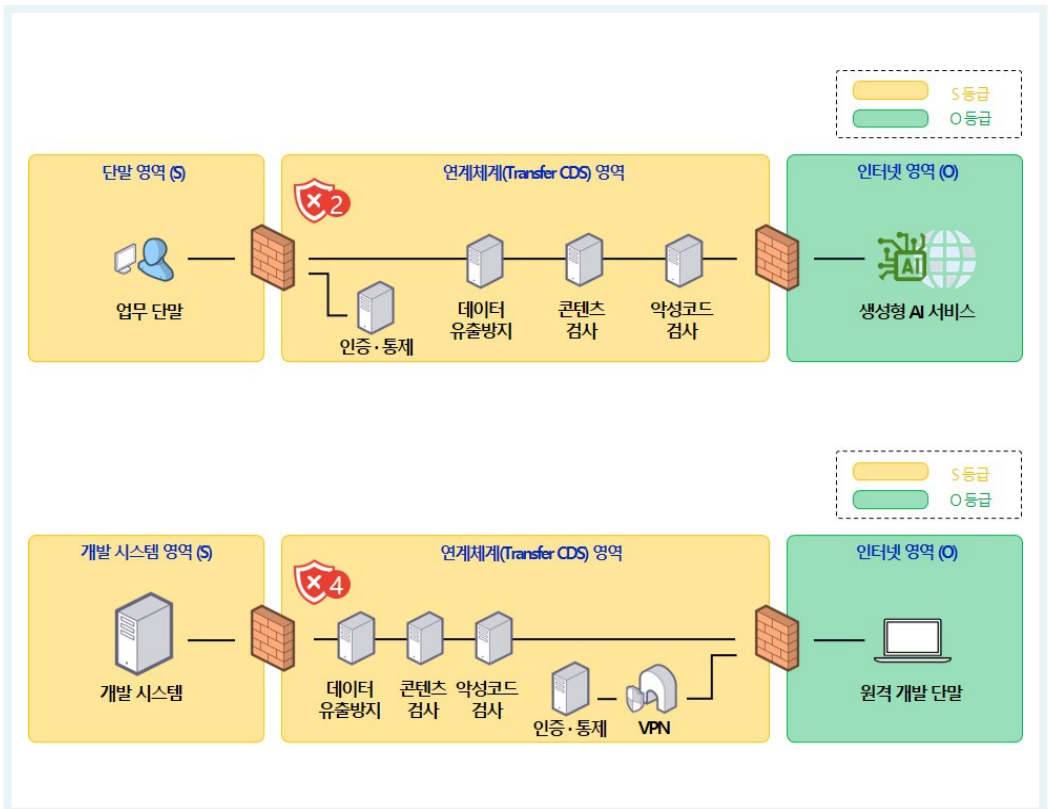
또한, 기관 전산망으로 유입되는 데이터 역시 정보의 보안등급 분류, 포맷 확인, 악성코드 검사, 콘텐츠 분석 등 엄격한 보안 절차가 요구된다. 수신되는 정보가 내부 업무시스템에 저장되기 전, AV 검사, DLP 분석, 포맷 필터링 등 기술적 통제를 거쳐야 하며, 허용되지 않은 포맷이나 탐지된 위험 요소가 있을 경우 전송은 거부된다. 수신 단말은 인증된 사용자 및 인가된 시스템에서만 허용되며, 정보 저장 위치, 처리 방식은 정책으로 명시되어야 한다.

Transfer CDS를 구성하는 본 정보서비스 모델은 예시이며, 기관 업무환경과 정보서비스 구축 시 업무 특성을 고려하여 Transfer CDS 구성 및 보안원칙 적용 과정을 수행해야 한다.

4. 보안위협 식별

Transfer CDS를 구성하는 정보서비스 예시는 업무 단말에서 생성형 AI 서비스를 활용하기 위한 모델과 원격지에서 원격 개발 단말을 통해 개발 시스템에 접속하는 모델로 구분하였으며, 〈표 4-2〉와 같이 정보서비스 모델 구성 중 연계체계(Transfer CDS)를 대상으로 보안 위협을 식별한다.

그림 4-4 Transfer CDS 보안위협 대상 식별



Transfer CDS를 구성하는 본 정보서비스 모델은 예시이며, 기관 업무환경 및 정보서비스 특성을 고려하여 Transfer CDS 구축·운영 시 환경구성 및 보안위협 대상을 식별해야 한다.

표 4-2 Transfer CDS 보안 위협

대상	구분	보안위협 번호	보안위협 요소
연계 체계	②, ④ Transfer CDS	TH-M11-11	연계체계 비인가 접근
		TH-M11-12	이용자 인증 우회
		TH-M11-13	비인가 정보 접근 및 유출
		TH-M11-14	비인가 보안 영역 접근
		TH-M11-15	보안 영역 간 비인가 네트워크 연결
		TH-M11-16	연계체계 인증 정보 유출
		TH-M11-17	관리자 기능 비인가 접근
		TH-M11-18	비인가 매체 연결 및 기능 실행
		TH-M11-19	취약점 노출 및 악용
		TH-M11-20	정보 접근 이력 변조

제3절

Transfer CDS 보안 요구사항 및 보안대책

기관은 국가 망 보안체계(N2SF) 정보서비스 모델의 안전한 활용을 위해 「정보 생산·저장」 및 「정보 이동」 보안원칙을 준수해야 하며, Transfer CDS를 구성한 정보서비스 구축·운영 시 연계 지점에서 보안위협을 식별하고 이에 대한 보안대책을 적용해야 한다.

정보서비스 구성요소 분석, 모델링 및 C/S/O 평가, 보안원칙 적용, 보안위협 식별 과정을 통해 위협을 파악하고, 정보서비스 모델 보안대책 수립 방향성과 국가·공공기관의 정책적 요구사항을 반영하여 보안 요구사항 및 N2SF 보안통제 항목을 선정하였다.

표 4-3 Transfer CDS 보안 요구사항 및 보안통제 항목

구분(유형)	구성요소	보안위협	보안 요구사항	N2SF 보안통제 항목
연계 체계	②, ④ Transfer CDS	(TH-M11-1) 연계체계 비인가 접근 (TH-M11-2) 이용자 인증 우회	Transfer CDS 비인가 접근 차단	N2SF-AC-1 N2SF-AC-1(1) N2SF-AC-1(2) N2SF-AC-1(3) N2SF-AC-1(4) N2SF-AC-3 N2SF-DA-3 N2SF-DA-4 N2SF-LI-1 N2SF-LI-2 N2SF-LI-4
		(TH-M11-3) 비인가 정보 접근 및 유출	Transfer CDS 데이터 접근 제어	N2SF-CD-1 N2SF-CD-2 N2SF-CD-3 N2SF-CD-4 N2SF-CD-5 N2SF-CD-6 N2SF-CD-7 N2SF-CD-8 N2SF-CD-9 N2SF-CD-10 N2SF-CD-12 N2SF-CD-13

구분(유형)	구성요소	보안위협	보안 요구사항	N2SF 보안통제 항목
				N2SF-CD-M1 N2SF-CD-M2 N2SF-CD-M3 N2SF-CD-M4
		(TH-M11-4) 비인가 보안 영역 접근 (TH-M11-5) 보안 영역 간 비인가 네트워크 연결	Transfer CDS 네트워크 제어	N2SF-IS-4 N2SF-IF-1 N2SF-IF-6 N2SF-IF-9 N2SF-EB-3
		(TH-M11-6) 연계체계 인증 정보 유출	Transfer CDS 인증 정보 보호	N2SF-AU-5 N2SF-AU-5(1) N2SF-AU-5(2) N2SF-AU-M1
		(TH-M11-7) 관리자 기능 비인가 접근 (TH-M11-8) 비인가 매체 연결 및 기능 실행	Transfer CDS 보안성 유지	N2SF-LP-1 N2SF-LP-4 N2SF-LP-4(1) N2SF-LP-4(4) N2SF-AC-1(5) N2SF-AC-3(1) N2SF-EB-8 N2SF-EB-10 N2SF-EB-11 N2SF-EB-13 N2SF-DV-4 N2SF-DV-6 N2SF-DV-10 N2SF-DV-12 N2SF-IN-1(1) N2SF-IN-5 N2SF-IN-6 N2SF-IN-11
		(TH-M11-9) 취약점 노출 및 악용 (TH-M11-10) 정보 접근 이력 변조	Transfer CDS 운용 관리	N2SF-LP-M1 N2SF-LP-M2 N2SF-AC-1(2) N2SF-AC-M1 N2SF-AC-M2 N2SF-AC-M3 N2SF-LI-M1 N2SF-LI-M2 N2SF-IS-2 N2SF-IF-M1 N2SF-IF-M2 N2SF-IF-M3 N2SF-IF-M4 N2SF-IF-M5 N2SF-EB-M5

1. Transfer CDS에 대한 보안요구사항 및 보안대책

Transfer CDS는 보안 영역 간 정보 접근이 필요한 경우에 안전한 접근을 중계·통제하는 핵심 보안 구성요소이다. Transfer CDS를 포함하는 정보서비스 모델에서는 Transfer CDS 접속 시부터 연결 종료 시까지 보안통제가 적용되어야 한다. 본 해설서에서는 Transfer CDS를 대상으로 보안요구사항 및 보안대책을 기술하며, 기관 환경 및 운영하고자 하는 정보서비스 특성을 고려하여 보안대책 수립을 검토해야 한다.

Transfer CDS가 구성된 정보서비스 구축·운영 시 다음과 같은 보안 요구사항 및 보안통제 항목을 적용해야 한다.

① 「Transfer CDS」 비인가 접근 차단

Transfer CDS는 사전 승인된 사용자 및 등록된 단말·시스템만 접근할 수 있도록 구성되어야 하며, 비인가된 단말·시스템이나 변조된 애플리케이션을 통한 접근은 인증 단계에서 차단해야 한다. 인증되지 않은 접근은 세션 생성 이전에 탐지 및 차단되어야 한다.

② 「Transfer CDS」 데이터 접근 제어

Transfer CDS를 통한 데이터 흐름은 업무 등급(S·O 등급) 간의 구간을 넘나들므로, 데이터 열람 시 메타데이터 및 데이터 본문의 불필요한 확산을 막고, 열람 종료 시 모든 캐시·임시 데이터는 자동 삭제되어야 한다. 동시에, 접근한 정보에 대해 다운로드, 복사, 인쇄, 화면 캡처 등은 통제되어야 하며, 정보 흐름은 로깅되어야 한다.

Transfer CDS는 인증 후, 업무 역할 및 유형에 따라 접근 가능한 데이터 등급(S등급, O등급)을 분리·통제해야 한다. 필요 최소한의 접근 권한만을 부여하며, 인증된 단말·시스템이라도 허가받지 않은 상위 보안등급 정보는 접근이 제한되어야 한다.

③ 「Transfer CDS」 네트워크 제어

Transfer CDS 인증 우회 시도 및 사전 승인된 기관 전산망 외 비인가 네트워크로의 접근을 차단해야 한다.

Transfer CDS를 통해 보안 영역 간의 통신을 연계해야 하며, 직접적인 네트워크 연결은 물리적·논리적으로 차단 등 보안대책을 적용해야 한다. Transfer CDS가 요청 및 응답을 중계·검증함으로써 상호 신뢰 수준을 조정하는 통제점이 되어야 한다.

비인가 네트워크 프로토콜은 차단해야 한다.

Transfer CDS는 연결 세션의 생성·유지·종료를 실시간으로 통제하며, 일정 시간 이상 비활동 시 자동 연결 종료 처리되어야 한다. 생성된 세션의 모든 요청·응답 흐름은 감사 로그로 저장되며, 해당 로그는 위·변조되지 않도록 안전하게 보관되어야 한다.

④ 「Transfer CDS」 인증 정보 보호

Transfer CDS 이용자 및 단말·시스템 인증 정보 변경에 대한 관리 정책을 수립하여, 무단 변경 등을 방지해야 한다.

Transfer CDS 인증 정보가 유출되지 않도록 정보 관리 정책을 수립해야 하며, 인증 정보 유출 시 대응 절차를 마련해야 한다.

⑤ 「Transfer CDS」 보안성 유지

Transfer CDS 관리자 권한 계정을 일반 사용자 계정과 분리하여 관리해야 하며, 비인가 장치의 연결 등을 통제해야 한다.

Transfer CDS의 취약점으로 인해 보안위협이 발생하지 않도록 최신 보안 업데이트 등 보안성을 유지해야 한다.

Transfer CDS에 비인가 기능·소프트웨어의 설치·실행 및 비인가 형상 변경으로 인한 보안위협이 발생하지 않도록 형상관리 등을 수행해야 한다.

그 외 기관 업무환경에 필요한 Transfer CDS의 보안 조치가 완료되어야 한다.

⑥ 「Transfer CDS」 운용 관리

Transfer CDS의 관리자 기능은 최소 권한 사용자만 접근 가능해야 하며, 관리자 작업 이력(로그인 시각, 설정 변경, 정책 적용 등)은 모두 기록되어야 한다. 설정 변경, 사용자 등록, 시스템 업데이트 등 주요 기능 실행에 대한 2인 승인 및 검토 절차가 마련되어야 한다.

Transfer CDS의 모든 접근 및 흐름 기록은 정보보안담당자가 주기적으로 확인할 수 있도록 로그로 저장되고, 로그 접근 권한은 분리되어야 하며, 삭제·변경은 시스템적으로 제한되어야 한다.

기관은 위와 같은 보안 요구사항 및 〈표 4-4〉의 보안통제 항목을 포함하는 보안대책을 준수해야 한다.

표 4-4 Transfer CDS 보안통제 항목

코드	보안통제 항목	내용
① Transfer CDS 비인가 접근 차단		
N2SF-AC-1	계정 관리 자동화	• 정보시스템 계정 관리를 효율화하고, 인적 오류를 최소화하기 위해 자동화된 메커니즘을 사용하여 계정 관리를 수행한다.
N2SF-AC-1(1)	동적 계정 관리	• 사용자 상태(입사, 퇴사, 부서 이동 등)에 따라 계정 정보를 실시간으로 반영하고, 시스템 간 계정 동기화를 통해 계정 수명주기 관리를 자동화한다.
N2SF-AC-1(2)	계정 상태 모니터링	• 계정의 임시 생성, 수정, 활성화, 비활성화 및 삭제 등을 모니터링한다.
N2SF-AC-1(3)	계정 자동 비활성화	• 계정 사용 기간이 종료되거나 일정 기간 미사용된 계정은 자동으로 비활성화한다.
N2SF-AC-1(4)	계정 자동 로그아웃	• 비활동 시간이 일정 기간 지속되었을 때 정보시스템에서 자동 로그아웃 되어야 한다.
N2SF-AC-3	의심스러운 계정 모니터링	• 비정상적이거나 의심스러운 계정 접속 시도 및 활동을 지속적으로 모니터링한다.
N2SF-DA-3	단말 식별 및 인증	• 단말의 고유 식별자(MAC, TPM, 인증서 등)를 통해 단말을 식별하고, 등록된 단말만 인증을 통해 시스템에 접근할 수 있도록 한다.
N2SF-DA-4	인증된 단말의 접속 관리	• 인증된 단말이라 하더라도 접속 시간, 위치, 사용자에 따라 세부 접근 권한을 제어하고, 접근 이력을 기록하여 감사 가능하도록 한다.
N2SF-LI-1	유효한 인증정보 노출 방지	• 인증 과정에서 유효한 인증 정보가 노출되지 않도록 한다.
N2SF-LI-2	로그인 실패에 따른 접속 제한	• 정의한 횟수 이상 연속적으로 로그인을 실패한 경우 일정시간 계정을 차단(또는 잠김)하거나 접속을 제한한다.
N2SF-LI-4	계정 잠금 해제 인증요소 추가	• 계정 잠금 상태에서 해제 요청 시 기본 인증 요소 외 인증요소를 추가 사용한다.
② Transfer CDS 데이터 접근 제어		
N2SF-CD-1	도메인 간 정보 흐름 검증 및 통제	• 서로 다른 보안 도메인 간 정보 흐름 시 데이터 유형, 등급, 출처를 검증하고 사전에 정의된 정책에 따라 전송을 허용, 차단 또는 보류한다.
N2SF-CD-2	다단계 보안 레이블 적용	• 전송되는 정보에 대해 다단계 보안 등급(예: 기밀, 민감, 공개)을 태깅하고, 대상 도메인의 수신 허용 기준에 부합하는 경우에만 전달한다.
N2SF-CD-3	일방향 전송 기술 적용 (Data Diode)	• 정보 유출 방지를 위해 단방향 전송 장치(Data Diode)를 활용하여 물리적 또는 논리적 단방향 정보 흐름을 강제한다. ※ N2SF-IF-5와 유사하지만, CDS에서 일방향 보장 장비 사용 시 구체적으로 분리 필요
N2SF-CD-4	검증 기반 릴레이 시스템 적용	• 수신된 정보는 릴레이 서버를 통해 악성코드 스캔, 포맷 검증, 콘텐츠 정제 후 안전성 판단을 거쳐 송신된다.
N2SF-CD-5	파일 유형 기반 전송 정책	• 파일 확장자, MIME 타입, 내부 Magic Number 등을 기준으로 허용된 파일 유형만 송수신 허용하고 나머지는 격리 또는 삭제한다.
N2SF-CD-6	콘텐츠 무해화 (CDR) 적용	• 전송 전 파일 내 삽입된 숨겨진 객체, 매크로, 스크립트 등을 제거하고 안전한 형식으로 변환하여 콘텐츠를 정제한다.

코드	보안통제 항목	내용
N2SF-CD-7	메타데이터 기반 통제 정책	• 파일 메타데이터의 생성일, 작성자, 등급 등 정보에 따라 송수신 정책을 달리 적용하고, 필요 시 메타데이터 제거 후 전송한다.
N2SF-CD-8	승인된 CDS 구성요소만 사용	• 크로스 도메인 연계를 위한 CDS는 기관이 검증하고 승인한 하드웨어/소프트웨어 구성요소만을 사용해야 한다.
N2SF-CD-9	CDS 우회 경로 탐지 및 차단	• CDS를 우회하여 다른 경로(USB, 무선, 별도 링크 등)로 도메인 간 전송을 시도하는 행위를 탐지하고 차단한다.
N2SF-CD-10	전송 실패 보호 및 무결성 보장	• 전송 중 실패 시 데이터가 잔존하거나 일부가 누락되지 않도록 조치하고, 수신자가 정보의 완전성과 무결성을 검증할 수 있도록 한다.
N2SF-CD-12	사용자 및 단말 등록 기반 접근 제어	• CDS 접근을 허용할 사용자와 단말 정보를 사전에 등록하고, 정책에 기반해 인증을 수행한다.
N2SF-CD-13	트래픽 흐름 컨텍스트 분석	• 동일 사용자·단말의 연속적인 전송 흐름을 분석하여 비정상 컨텍스트(다량, 시간외 등)를 차단한다.
N2SF-CD-M1	CDS 운용 정책 수립	• CDS 구성, 운용, 접근, 예외 처리 절차 등을 포함한 관리 정책을 수립하고 주기적으로 갱신한다.
N2SF-CD-M2	CDS 통제 로그 기록 및 감사	• CDS를 통한 정보 흐름의 허용, 차단, 예외처리 등의 모든 활동을 로깅하고 주기적으로 감사한다.
N2SF-CD-M3	도메인 간 정보 교환 승인 프로세스	• 도메인 간 정보 교환은 사전 승인된 업무 목적 및 사용자에 한정되며, 자동화된 승인 및 검토 체계를 갖추어야 한다.
N2SF-CD-M4	CDS 구성요소 무결성 검증	• CDS 시스템의 구성요소(소프트웨어, 펌웨어 등)에 대한 무결성을 정기적으로 검증하고 변경 시 승인 절차를 거친다.
③ Transfer CDS 네트워크 제어		
N2SF-IS-4	네트워크 격리	• 내부망, 외부망, 보안망 등 네트워크 간에 방화벽, 라우팅 제어 등으로 트래픽을 분리하여 정보 유출 또는 확산을 방지한다.
N2SF-IF-1	정보흐름의 동적 통제	• 정보시스템의 비정상 동작, 외부의 공격 등 지정한 조건에 대하여 정보흐름을 동적으로 통제한다.
N2SF-IF-6	필터링 규칙 정보흐름 통제	• 보안 및 프라이버시 등에 관한 필터링 규칙을 적용하여 정보흐름을 통제한다.
N2SF-IF-9	출발지점과 도착지점 식별 및 인증	• 정보 전송 시 개인, 기관, 응용프로그램 혹은 정보시스템 등 하나 이상을 사용하여 출발지점과 도착지점을 식별하고 인증한다.
N2SF-EB-3	화이트리스트 기반 통신 허용	• 기본적으로 모든 통신을 차단한 상태에서 필요한 통신만을 허용하는 화이트리스트 기반 정책을 적용한다.
④ Transfer CDS 인증 정보 보호		
N2SF-AU-5	인증 시스템 구성 및 관리	• 인증 시스템의 구성 요소를 안전하게 설정하고 변경 시 보안에 영향이 없도록 관리한다.
N2SF-AU-5(1)	비밀번호 보안수준 점검	• 자동화된 도구를 이용하여 비밀번호 정책에 적합하게 설정·유지되고 있는지 점검한다.
N2SF-AU-5(2)	대체 보안수단 강구	• 보안 기능을 구현 또는 제공하는 주요 수단을 사용할 수 없거나 손상되었을 상황을 대비한 대체 보안수단을 강구한다.
N2SF-AU-M1	인증 정보 접근 권한 통제 및 관리	• 인증 정보는 최소한의 인원만 접근할 수 있도록 제한하고 기록을 남긴다.

코드	보안통제 항목	내용
⑤ Transfer CDS 보안성 유지		
N2SF-LP-1	정보시스템 접근 권한 정의	• 업무정보(데이터)를 식별하고, 업무정보를 저장하고 있는 정보시스템 접근 권한을 정의한다.
N2SF-LP-4	관리자 권한 제한	• 정보시스템 접근에 필요한 최소한의 관리자 및 운영자 등에게만 관리자 권한을 부여한다.
N2SF-LP-4(1)	원격접속을 통한 관리자 권한 접속제한	• 기관 네트워크 내부에서 관리자 권한 접속이 제한되는 경우 등 불가피한 상황에서만 한시적으로 기관 네트워크 외부에서의 관리자 권한 접속을 허용하며, 목적이 달성된 경우 외부에서의 관리자 권한 접속을 즉시 차단한다.
N2SF-LP-4(4)	관리자 권한 실행 로깅 및 감사	• 관리자 권한 기능 실행 내역은 로깅하고 주기적인 사용 내역 감사를 실시한다.
N2SF-AC-1(5)	불필요한 관리자 권한 계정 제거	• 관리자 권한이 필요 없거나 활용이 종료된 계정은 비활성화 또는 삭제 조치한다.
N2SF-AC-3(1)	위험에 노출된 계정 비활성화	• 정보시스템 위협 탐지 시, 위협에 노출된 계정은 신속히 비활성화하거나 제한 조치를 한다.
N2SF-EB-8	운영관리용 포트의 물리적 연결 차단	• 운영관리용 포트에 인가되지 않은 장치의 포트 연결을 차단한다.
N2SF-EB-10	정보시스템 구성요소 외부 노출 차단	• 정보시스템 운영관리 및 서비스를 제공하는 구성요소가 외부 노출되지 않도록 차단한다.
N2SF-EB-11	외부 경계 보호 기능 유지	• 외부 경계를 보호하는 정보자산(보안시스템 등) 장애 시에도 보호기능은 유지되도록 구성한다.
N2SF-EB-13	오류정보 발신자 전송 제한	• 네트워크 규약에 따른 통신 오류 발생 시 발신자에게 피드백이나 경고를 통해 정보시스템 구성이나 취약점이 전송되지 않도록 한다.
N2SF-DV-4	포트 및 입출력 장치 제어	• 정보시스템의 포트나 입출력 장치를 제어하여 악성코드 유입 및 정보 유출을 차단한다.
N2SF-DV-6	통신 기능이 포함된 저장장치 제한	• 통신기능이 포함된 저장장치를 사용을 제한한다.
N2SF-DV-10	저장장치 연결 금지	• 정보시스템 기동 및 종료 또는 재시작하는 동안 쓰기 가능한 저장장치 연결을 금지한다.
N2SF-DV-12	장치 펌웨어 업데이트 검증	• 펌웨어 업데이트 시 서명 검증 또는 위변조 여부를 검증하여 설치를 제한한다.
N2SF-IN-1(1)	정보시스템 구성요소 최신상태 유지	• 정보시스템 내의 모든 구성요소가 포함되도록 정보시스템 구성 요소 목록을 작성하고 정기적으로 검토 및 최신 상태로 업데이트 한다.
N2SF-IN-5	비인가 변경 방지	• 인가되지 않은 정보시스템 구성요소 변경을 방지한다.
N2SF-IN-6	불필요한 구성요소 제거	• 필요 기능만 제공하도록 구성하고, 사용하지 않는 기능, 포트, 프로토콜, 소프트웨어, 서비스의 사용을 제거하거나 비활성화한다.
N2SF-IN-11	재기동 서비스 신뢰성 확보	• 정보시스템 구성요소와 서비스가 재기동(재부팅) 할 때 소프트웨어와 데이터는 신뢰된 곳으로부터 획득한다.

코드	보안통제 항목	내용
⑥ Transfer CDS 운용 관리		
N2SF-LP-M1	특별권한 사용자 지정	• 일반 사용 권한과 별도로 특별권한 사용자 그룹을 지정하고, 이들의 권한 부여와 변경을 통제한다.
N2SF-LP-M2	주요 사용자 위험 관리	• 주요 사용자의 권한과 활동을 모니터링하고 이상 징후를 탐지하여 위험을 사전에 관리한다.
N2SF-AC-1(2)	계정 상태 모니터링	• 계정의 임시 생성, 수정, 활성화, 비활성화 및 삭제 등을 모니터링한다.
N2SF-AC-M1	감사 활동 자동화	• 계정 사용 및 관련된 감사 활동을 자동화하여 관리
N2SF-AC-M2	감사기록 생성	• 계정 활동에 대한 감사 기록을 생성하여 보관 및 분석할 수 있도록 함
N2SF-AC-M3	세션 감사	• 세션 활동을 기록하고 주기적으로 감사하여 비정상적 행위 탐지
N2SF-LI-M1	로그인 실패 모니터링 및 보고	• 반복 실패, 의심 로그인 시도 등의 실패 패턴을 실시간 감지하고 관리자에게 보고
N2SF-LI-M2	주기적 로그인 정보 무결성 점검	• 로그인 관련 데이터(세션, 토큰, 사용자 매핑 정보 등)에 대해 주기적인 무결성 점검 및 이상 여부 확인
N2SF-IS-2	정보시스템 운영·관리 기능 표출 제한	• 일반 사용자에게 정보시스템 관리와 관련된 기능 및 인터페이스 표출을 제한한다.
N2SF-IF-M1	정보흐름 통제 정책 수립 및 갱신	• 정보 흐름에 대한 통제 기준 및 예외 절차를 문서화하고 정기적으로 갱신한다.
N2SF-IF-M2	정보흐름 로그 기록 및 보존	• 정보 흐름 통제 활동(허용/차단 등)을 로깅하고, 법적/감사 목적으로 일정 기간 보관한다.
N2SF-IF-M3	정보흐름 통제 감사 및 이행 점검	• 정보 흐름 통제의 적용 현황을 정기적으로 점검하여 정책 미준수 사항 식별 및 개선
N2SF-IF-M4	비인가 흐름 탐지 자동화	• 정책을 우회하거나 비정상적 흐름을 탐지하기 위한 자동화 도구 또는 시스템 구축
N2SF-IF-M5	통제 실패·예외 보고 체계	• 통제가 실패하거나 예외 발생 시 담당자에게 자동 보고하고 이를 기록하는 체계를 마련한다.
N2SF-EB-M5	비상 시 외부 통신 격리	• 침해 발생 시 외부 통신을 즉시 차단할 수 있는 절차를 마련한다.

2. Transfer CDS 연계에 대한 보안 요구사항 및 보안대책

Transfer CDS를 구성한 정보서비스 모델에서는 Transfer CDS과 연계하는 보안 영역의 단말, 시스템 등에 대한 보안대책 적용이 필요하다. 본 해설서에서 기술한 정보서비스 모델은 예시이며, 기관이 구축·운영하고자 하는 정보서비스의 업무 목적 및 특성을 고려하여 단말·시스템의 보안성 유지, 인증, 운영 관리, 네트워크 통제 등 보안 요구사항 및 보안통제 항목을 적용해야 한다.

제5장

MLS CDS

제1절 MLS CDS

제1절

MLS CDS

MLS CDS(Multi Level Security CDS)는 단일 시스템 환경 내에서 다양한 보안 등급의 정보와 사용자가 혼재할 때, 사용자의 인가 등급에 맞는 정보에만 접근하도록 강제하는 고도의 보안 솔루션이다. 이는 높은 보안 수준을 요구하는 환경에서 정보의 불법적인 접근과 유출을 원천적으로 방지하기 위해 사용된다.

MLS CDS 환경에서 Access CDS는 원본 데이터의 물리적 이동이나 복제를 허용하지 않고, 인가된 이용자가 자신의 보안 등급에 따라 필요한 정보만 열람할 수 있도록 보안 통제를 적용한다. 이를 위해 프로토콜 분리와 화면 기반 정보 스트리밍 기술이 사용되며, 사용자는 정책이 허용하는 범위 내에서만 정보를 열람할 수 있다. 이러한 방식은 다중 보안 등급이 공존하는 단일 시스템 내에서도, 원본 데이터의 보호와 이용자별 안전한 활용을 동시에 보장한다는 점에서 핵심적인 의미를 가진다.

MLS CDS 환경에서 Transfer CDS는 서로 다른 보안 등급 간의 데이터 이동이나 정보 흐름을 다룬다. 이때 읽기(Read)/쓰기(Write) 규칙을 보안 정책에 따라 적용하여, 높은 등급의 정보가 낮은 등급으로 유출되거나 낮은 등급의 정보가 높은 등급의 정보에 부적절하게 기록되지 않도록 제어한다. 즉, 정보의 흐름 방향성에 보안 통제를 부여하여 안전한 전송을 보장한다.

이와 같이 MLS CDS는 운영체제 또는 하드웨어 수준에서 강제적 접근 통제(MAC, Mandatory Access Control)기반 정책 엔진을 통해 Access CDS와 Transfer CDS를 상황에 맞게 적용함으로써, 단일 시스템 환경에서도 다중 보안 등급 데이터를 안전하게 활용할 수 있도록 보장한다. 시스템 내의 모든 정보 또는 사용자·정보시스템 등에 각각 보안 등급을 나타내는 레이블(Label)이 부여되고, MLS CDS는 이를 기반으로 정보 접근과 전송을 통제한다.

또한, MLS CDS는 서로 다른 등급의 정보가 하나의 시스템에 존재하더라도 물리적으로 분리된 것처럼 완벽한 격리를 보장하는 기능을 제공한다. 예를 들어, 단일 지휘 통제 단말기에서 암호화된 아군 위치(비밀)와 기상 정보(공개)를 동시에 조회할 때, MLS CDS는 아군 위치가 기상 정보에 기록되지 않도록 모든 정보흐름을 감시하고 통제한다.

결론적으로 MLS CDS는 복수의 물리적 시스템을 구축하는 비용과 복잡성을 줄이고, 단일 플랫폼 내에서 다중 등급 데이터의 안전한 공존과 활용을 가능하게 하는 고도의 보안기술이 적용된 연계방식이다.

MLS CDS의 보안 위협과 보안 요구사항은 정보에 대한 열람 측면에서는 Access CDS와 보안등급 간 정보 흐름 통제는 Transfer CDS를 융합하여 정의할 수 있다.

다음 그림은 원격지 단말(O등급)에서 MLS CDS 연계체계를 통해 S등급 업무시스템과 O등급 업무시스템이 공존하는 영역에 접근하여 등급에 따른 차등적인 권한 통제에 따라 접속 및 정보를 활용하는 것으로 Access CDS와 Transfer CDS의 보안통제를 동시에 구현한 예시이다.

그림 5-1 MLS CDS 정보서비스 구성요소 분석

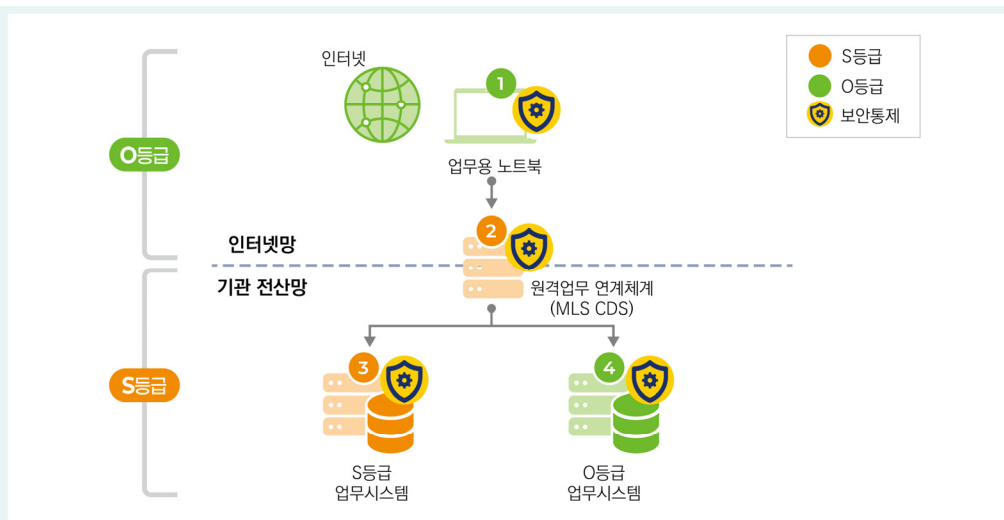
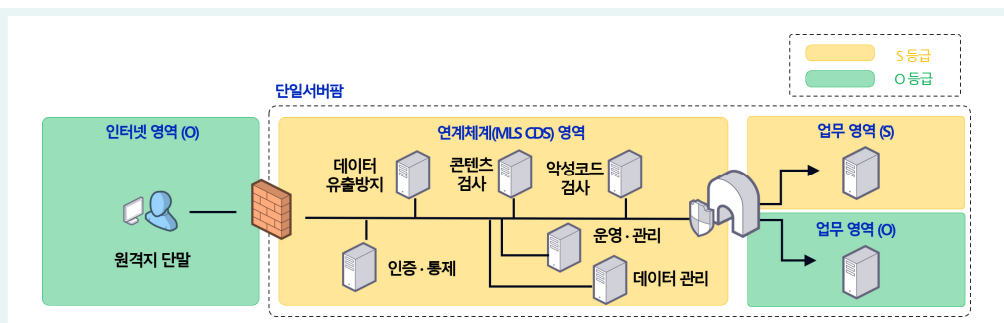


그림 5-2 MLS CDS 사용



1.0

국가 망 보안체계
보안 가이드라인

정보서비스 모델 해설서 모델 11. 정보 연계를 위한 CDS 구성

부록 2-11