

대분류/20  
정보통신

중분류/01  
정보기술

소분류/02  
정보기술개발

세분류/06  
보안엔지니어링

능력단위/14

NCS학습모듈

# 네트워크 보안 구축

LM2001020614\_16v3



교육부

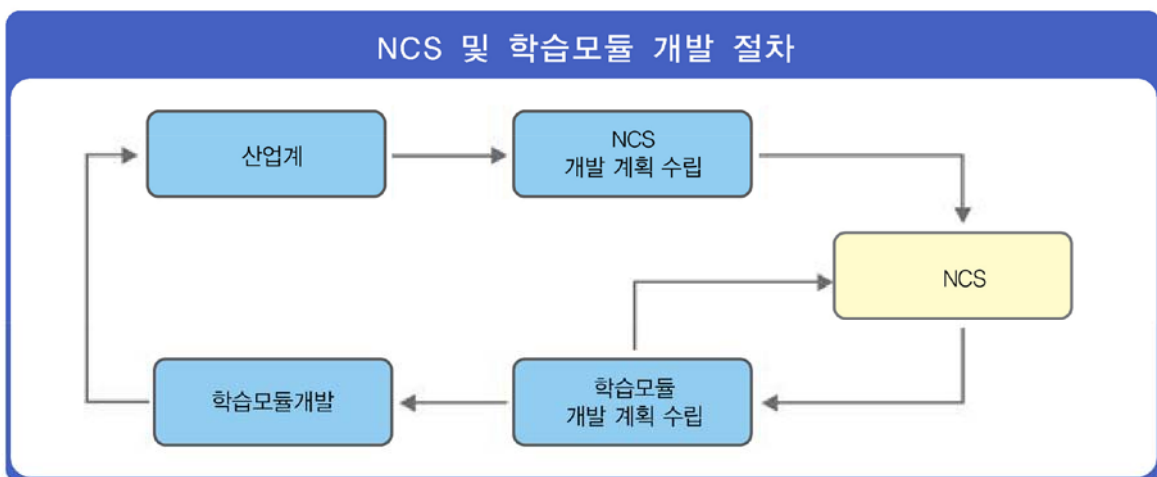
NCS 학습모듈은 교육훈련기관에서 출처를 명시하고 교육적 목적으로 활용할 수 있습니다. 다만 NCS 학습모듈에는 국가(교육부)가 저작권 일체를 보유하지 않은 저작물들(출처가 표기되어 있는 도표, 사진, 삽화, 도면 등)이 포함되어 있으므로 이러한 저작물들의 변형, 복제, 공연, 배포, 공중 송신 등과 이러한 저작물들을 활용한 2차 저작물의 생성을 위해서는 반드시 원작자의 동의를 받아야 합니다.

## NCS 학습모듈의 이해

※ 본 학습모듈은 「NCS 국가직무능력표준」 사이트(<http://www.ncs.go.kr>) 에서 확인 및 다운로드 할 수 있습니다.

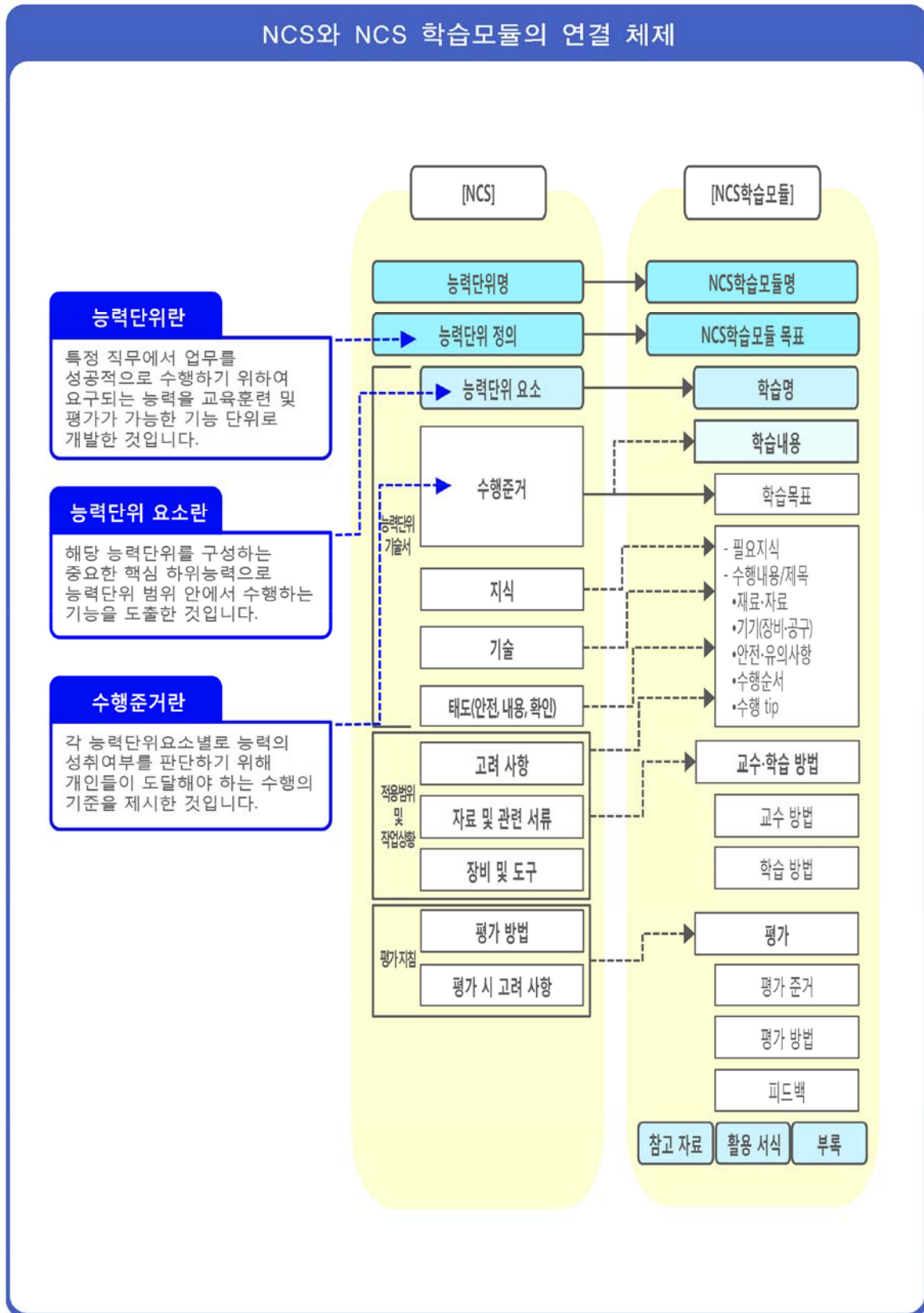
### (1) NCS 학습모듈이란?

- 국가직무능력표준(NCS: National Competency Standards)이란 산업현장에서 직무를 수행하기 위해 요구되는 지식·기술·소양 등의 내용을 국가가 산업부문별·수준별로 체계화한 것으로 산업현장의 직무를 성공적으로 수행하기 위해 필요한 능력(지식, 기술, 태도)을 국가적 차원에서 표준화한 것을 의미합니다.
- 국가직무능력표준(이하 NCS)이 현장의 ‘직무 요구서’라고 한다면, NCS 학습모듈은 NCS의 능력단위를 교육훈련에서 학습할 수 있도록 구성한 ‘교수·학습 자료’입니다. NCS 학습모듈은 구체적인 직무를 학습할 수 있도록 이론 및 실습과 관련된 내용을 상세하게 제시하고 있습니다.



- NCS 학습모듈은 다음과 같은 특징을 가지고 있습니다.
- 첫째, NCS 학습모듈은 산업계에서 요구하는 직무능력을 교육훈련 현장에 활용할 수 있도록 성취목표와 학습의 방향을 명확히 제시하는 가이드라인의 역할을 합니다.
- 둘째, NCS 학습모듈은 특성화고, 마이스터고, 전문대학, 4년제 대학교의 교육기관 및 훈련기관, 직장교육기관 등에서 표준교재로 활용할 수 있으며 교육과정 개편 시에도 유용하게 참고할 수 있습니다.

- NCS와 NCS 학습모듈 간의 연결 체제를 살펴보면 아래 그림과 같습니다.



## (2) NCS 학습모듈의 체계

- NCS 학습모듈은 1.학습모듈의 위치, 2.학습모듈의 개요, 3.학습모듈의 내용 체계, 4.참고 자료, 5.활용 서식/부록 으로 구성되어 있습니다.

### 1. NCS 학습모듈의 위치

- NCS 학습모듈의 위치는 NCS 분류 체계에서 해당 학습모듈이 어디에 위치하는지를 한 눈에 볼 수 있도록 그림으로 제시한 것입니다.

예시 : 이·미용 서비스 분야 중 네일미용 세분류

### NCS-학습모듈의 위치

대분류	이용·숙박·여행·오락·스포츠
중분류	이·미용
소분류	아미용 서비스

세분류	능력단위	학습모듈명
헤어미용	네일 샵 위생 서비스	네일샵 위생서비스
피부미용	네일 화장을 제거	네일 화장을 제거
메이크업	네일 기본 관리	네일 기본관리
네일미용	네일 랩	네일 랩
이용	네일 팁	네일 팁
	젤 네일	젤 네일
	아크릴릭 네일	아크릴 네일
	평면 네일아트	평면 네일아트
	융합 네일아트	융합 네일아트
	네일 샵 운영관리	네일샵 운영관리

#### 학습모듈은

NCS 능력단위 1개당 1개의 학습모듈 개발을 원칙으로 합니다. 그러나 필요에 따라 고용 단위 및 교과단위를 고려하여 능력단위 몇 개를 묶어서 1개의 학습모듈로 개발할 수 있으며, NCS 능력단위 1개를 여러 개의 학습모듈로 나누어 개발할 수도 있습니다.

## 2. NCS 학습모듈의 개요

### 구 성

- NCS 학습모듈 개요는 학습모듈이 포함하고 있는 내용을 개략적으로 설명한 것으로서 **학습모듈의 목표**, **선수 학습**, **학습모듈의 내용 체계**, **핵심 용어**로 구성되어 있습니다.

학습모듈의 목표	해당 NCS 능력단위의 정의를 토대로 학습목표를 작성한 것입니다.
선수 학습	해당 학습모듈에 대한 효과적인 교수·학습을 위하여 사전에 이수해야 하는 학습모듈, 학습 내용, 관련 교과목 등을 기술한 것입니다.
학습모듈의 내용 체계	해당 NCS 능력단위요소가 학습모듈에서 구조화된 방식을 제시한 것입니다.
핵심 용어	해당 학습모듈의 학습 내용, 수행 내용, 설비·기자재 등 가운데 핵심적인 용어를 제시한 것입니다.

### 활 용 안 내

예시 : 네일미용 세분류의 ‘네일 기본관리’ 학습모듈

#### 네일 기본관리 학습모듈의 개요

##### 학습모듈의 목표

고객의 네일 보호와 미적 요구 충족을 위하여 효과적인 네일 관리로 프리에지 형태 만들기, 큐티를 정리하기, 컬러링하기, 보습제 도포하기, 마무리를 할 수 있다.

##### 선수학습

네일습 위성서비스(LM1201010401\_14v2)

##### 학습모듈의 내용체계

학습	학습 내용	NCS 능력단위 요소	
		코드번호	요소 명칭
1. 프리에지 형태 만들기	1-1. 네일 파일에 대한 이해와 활용 1-2. 프리에지 형태 파일링	1201010403_12v2.1	프리에지 모양 만들기
2. 큐티를 정리하기	2-1. 네일 기본관리의 매뉴얼 이해 2-2. 큐티를 관리	1201010403_14v2.2	큐티를 정리하기
3. 컬러링하기	3-1. 컬러링 매뉴얼 이해 3-2. 컬러링 방법 선정과 작업 3-3. 쉘 컬러링 작업	1201010403_14v2.3	컬러링
4. 보습제 도포하기	4-1. 보습제 선정과 도포 4-2. 각질제거	1201010403_14v2.4	보습제 바르기
5. 네일 기본관리 마무리하기	5-1. 유분기 제거 5-2. 네일 기본관리의 마무리와 정리	1201010403_14v2.5	마무리하기

##### 핵심 용어

프리에지, 니퍼, 큐서, 폴리시, 네일 파일, 스웨이형, 스웨이 오드형, 라운드형, 오발형, 포인트형

##### 학습모듈의 목표는

학습자가 해당 학습모듈을 통해 성취해야 할 목표를 제시한 것으로, 교수자는 학습자가 학습모듈의 전체적인 내용흐름을 파악할 수 있도록 지도하는 것이 필요합니다.

##### 선수 학습은

교수자나 학습자가 해당 모듈을 교수 또는 학습하기 이전에 이수해야 할 학습내용, 교과목, 핵심 단어 등을 표기한 것입니다. 따라서 교수자는 학습자가 개별 학습, 자기 주도 학습, 방과 후 활동 등 다양한 방법을 통해 이수할 수 있도록 지도하는 것이 필요합니다.

##### 핵심 용어는

학습모듈을 통해 학습되고 평가되어야 할 주요 용어입니다. 또한 당해 모듈 또는 타 모듈에서도 핵심 용어를 사용하여 학습내용을 구성할 수 있으며, 「NCS 국가 직무능력표준」 사이트([www.ncs.go.kr](http://www.ncs.go.kr))에서 색인(찾아보기) 중 하나로 이용할 수 있습니다.



### 3. NCS 학습모듈의 내용 체계

#### 구 성

- NCS 학습모듈의 내용은 크게 **학습**, **학습 내용**, **교수·학습 방법**, **평가** 로 구성되어 있습니다.

학습	해당 NCS 능력단위요소 명칭을 사용하여 제시한 것입니다. 학습은 크게 학습 내용, 교수·학습 방법, 평가로 구성되며 해당 NCS 능력단위의 능력단위 요소별 지식, 기술, 태도 등을 토대로 학습 내용을 제시한 것입니다.
학습 내용	학습 내용은 학습 목표, 필요 지식, 수행 내용으로 구성하였으며, 수행 내용은 재료·자료, 기기(장비·공구), 안전·유의 사항, 수행 순서, 수행 tip으로 구성한 것입니다. 학습모듈의 학습 내용은 업무의 표준화된 프로세스에 기반을 두고 실제 산업현장에서 이루어지는 업무활동을 다양한 방식으로 반영한 것입니다.
교수·학습 방법	학습 목표를 성취하기 위한 교수자와 학습자 간, 학습자와 학습자 간의 상호 작용이 활발하게 일어날 수 있도록 교수자의 활동 및 교수 전략, 학습자의 활동을 제시한 것입니다.
평가	평가는 해당 학습모듈의 학습 정도를 확인할 수 있는 평가 준거, 평가 방법, 평가 결과의 피드백 방법을 제시한 것입니다.

#### 활 용 안 내

예시 : 네일미용 세분류의 ‘네일 기본관리’ 학습모듈의 내용

학습 1	프리에지 형태 만들기(LM1201010403_14v2.1)
학습 2	큐티를 정리하기(LM1201010403_14v2.2)
<b>학습 3</b>	<b>컬러링하기(LM1201010403_14v2.3)</b>
학습 4	보습제 도포하기(LM1201010403_14v2.4)
학습 5	네일 기본관리 마무리하기(LM1201010403_14v2.5)

#### 학습은

해당 NCS 능력단위요소 명칭을 사용하여 제시하였습니다.  
학습은 일반교과의 ‘대단원’에 해당되며, 모듈을 구성하는 가장 큰 단위가 됩니다. 또한 완성된 직무를 수행하기 위한 가장 기본적인 단위로 사용할 수 있습니다.

#### 학습내용은

요소 별 수행준거를 기준으로 제시하였습니다. 일반교과의 ‘중단원’에 해당합니다.

#### 학습목표는

모듈 내의 학습내용을 이수했을 때 학습자가 보여줄 수 있는 행동수준을 의미합니다. 따라서 일반 수업시간의 과목목표로 활용할 수 있습니다.

### 3-1. 컬러링 매뉴얼 이해

#### 학습목표

- 고객의 요구에 따라 네일 폴리시 색상과 점착을 막기 위한 베이스코트를 아주 얇게 도포할 수 있다.
- 작업 매뉴얼에 따라 네일 폴리시를 일찍 없이 균일하게 도포할 수 있다.
- 작업 매뉴얼에 따라 네일 폴리시 도포 후 컬러 보호와 광택 부여를 위한 톱코트를 바를 수 있다.

#### 필요 지식 /

##### ① 컬러링 매뉴얼

컬러링 작업 전, 아세트 또는 네일 폴리시 리무버를 사용하여 손톱표면과 큐티클 주변, 손톱 밑 부분까지 깨끗하게 유분기를 제거해야 한다. 컬러링의 순서는 Base coating 1회 → Polishing 2회 → 컬러수정 → Top coating 1회 → 최종수정의 순서로 한다. 베이스코트는 칠크를 방지하고 발림성 향상을 위해 가장 먼저 도포하며 컬러링의 마지막에 컬러의 유지와 광택을 위해 톱코트를 도포한다. 네일 보강제(Nail Strengthner)를 바를 시에는 베이스코트를 도포하기 전에 사용한다.

#### 필요지식은

해당 NCS의 지식을 토대로 해당 학습에 대한 이해와 성과를 높이기 위해 알아야 할 주요 지식을 제시하였습니다. 필요지식은 수행에 꼭 필요한 핵심 내용을 위주로 제시하여 교수자의 역할이 매우 중요하며, 이후 수행순서 내용과 연계하여 교수·학습으로 진행할 수 있습니다.

## 수행 내용 / 컬러링 매뉴얼 실습하기

### 재료·자료

- 컬러링 관련 네일 미용 자료들
- 정리바구니, 베이스코트, 네일 폴리시, 톱코트, 오렌지우드스티, 탈지면, 폴리시러무버, 디스펜서 등

### 기기(장비·공구)

- 키펙터, 빔 프로젝터, 스크린 등

### 안전·유의사항

- 컬러링 재료들의 냄새를 직접적으로 맡지 않도록 유의한다.
- 컬러링 제품들이 대부분 유리병에 들어 있기 때문에 깨지지 않도록 각별히 조심한다.
- 컬러링 제품들은 상온에 마르기 때문에 개봉 후 뚜껑을 잘 닫도록 한다.

### 수행 순서

#### Ⅰ 네일 폴리시를 바르게 잡는다.

1. 손바닥에 네일 폴리시를 놓고 약지 소지를 이용하여 네일 폴리시를 잡는다.
2. 폴리시를 왼 손의 엄지와 검지로 고객의 작업손가락을 잡는다.
3. 폴리시를 왼 손의 중지 손가락을 굳게 펴서 발침대가 되도록 한다.
4. 반대편 손으로 네일 폴리시의 뚜껑을 열고 소지 손가락을 펴서 네일 폴리시를 왼 중지 손가락 위에 발쳐놓는다.
5. 다양한 형태의 폴리시를 잡아본다.

#### 수행 tip

- 흰색이 많이 섞인 네일 폴리시의 경우는 붓의 각도를 높이 세워 빠르게 브러시 작업을 해야 붓 자국이 나지 않는다.
- 컬러링은 기본 2회 정도이나 컬러에 따른 도료량과 컬러감에 따라 1~3회 사이로 증감할 수 있다.

## 수행 내용은

모듈에 제시한 것 중 기술(Skill)을 습득하기 위한 실습 과제로 활용할 수 있습니다.

## 재료·자료는

수행 내용을 수행하는데 필요한 재료 및 준비물로 실습 시 필요 준비물로 활용할 수 있습니다.

## 기기(장비·공구)는

수행 내용을 수행하는데 필요한 기본적인 장비 및 도구를 제시하였습니다. 제시된 기기 외에도 수행에 필요한 다양한 도구나 장비를 활용할 수 있습니다.

## 안전·유의사항은

수행 내용을 수행하는데 안전상 주의해야 할 점 및 유의 사항을 제시하였습니다. 수행 시 유념해야 하며, NCS의 고려사항도 추가적으로 활용할 수 있습니다.

## 수행 순서는

실습과제의 진행 순서로 활용할 수 있습니다.

## 수행 tip은

수행 내용에서 수행의 수월성을 높일 수 있는 아이디어를 제시하였습니다. 따라서 수행tip은 지도상의 안전 및 유의 사항 외에 전반적으로 적용되는 주안점 및 수행과제 목적에 대한 보충설명, 추가사항 등으로 활용할 수 있습니다.

## 학습3 교수·학습 방법

## 교수·학습 방법은

학습목표를 성취하는데 필요한 교수 방법과 학습 방법을 제시하였습니다.

### 교수 방법

- 컬러링 제품의 성분과 컬러별 질도의 차이, 베이스코트와 톱코트의 역할, 폴리시 잡는 방법, 큐어링 시간 등의 내용을 화면 자료와 함께 설명한다.
- 서식지를 활용하여 네일 컬러링 방법을 그림으로 그려 보게 한 뒤, 다양한 컬러링의 매뉴얼을 그려서 숙지하도록 한다.
- 셀 컬러링 시 주의사항을 계속 숙지시키도록 하며, 큐어링 시간에 대해 작성하도록 한다.

## 교수 방법은

해당 학습활동에 필요한 학습내용, 학습내용과 관련된 학습 자료명, 자료 형태, 수행내용의 진행 방식 등에 대하여 제시 하였습니다. 또한 학습자의 수업참여도를 제고하기 위한 방법 및 수업진행상 유의사항 등도 제시하였습니다. 선수학습이 필요한 학습을 학습자가 숙지하였는지 교수자가 확인하는 과정으로 활용할 수도 있습니다.

### 학습 방법

- 컬러링을 위한 재료의 필요성과 사용방법을 숙지하고 컬러링 매뉴얼 과정에 맞추어 작업 내용을 이해한다.
- 컬러링의 다양성에 대한 용어를 숙지하고 진행과정에 맞추어 내용을 작업한다.
- 셀 컬러링 시 적합한 큐어링 시간을 선택해서 큐어링 해본다.

## 학습 방법은

해당 학습활동에 필요한 학습자의 자기주도적 학습 방법을 제시하였습니다. 또한 학습자가 숙달해야 할 실기능력과 학습과정에서 주의해야 할 사항 등으로 제시하였습니다. 학습자가 학습을 이수하기 전에 반드시 숙지해야 할 기본 지식을 학습하였는지 스스로 확인하는 과정으로 활용할 수 있습니다.



## 학습3 평가

## 평가는

해당 NCS 능력단위 평가방법과 평가 시 고려 사항을 준용하여 작성하였습니다. 교수자 및 학습자가 평가항목 별 성취수준을 확인하는데 활용할 수 있습니다.

## 평가 준거

- 평가자는 학습자가 학습 목표를 성공적으로 달성하였는지를 평가해야 한다.
- 평가자는 다음 사항을 평가해야 한다.

학습내용	학습 목표	성취수준		
		상	중	하
필러링 매뉴얼 이해	고객의 요구에 따라 네일 폴리시 색상의 질감을 학기 위한 베이스코트를 아주 얇게 도포할 수 있다.			
	작업 매뉴얼에 따라 네일 폴리시를 얼룩 없이 균일하게 도포할 수 있다.			
	작업 매뉴얼에 따라 네일 폴리시 도포 후 컬러 보호와 광택 부여를 위한 톱코트를 바를 수 있다.			

## 평가 준거는

학습자가 해당 학습을 어느 정도 성취하였는지를 평가하기 위한 기준을 제시하고 있습니다. 학습목표와 연계하여 단위수업 시간에 평가항목 별 성취수준을 평가하는데 활용할 수 있습니다.

## 평가 방법은

NCS 능력단위의 평가방법을 준용하였으며, 평가 준거에 따른 평가방법을 2개 이상 제시하였습니다. 평가방법으로는 포트폴리오, 문제해결 시나리오, 서술형 시험, 논술형 시험, 사례연구, 평가자 체크리스트, 작업장 평가 등이 있으며, NCS의 능력단위 요소 별 수행 수준을 평가하는데 가장 적절한 방법을 선정하여 활용할 수 있습니다.

## 평가 방법

- 작업장 평가

학습내용	평가 항목	성취수준		
		상	중	하
필러링 매뉴얼 이해	고객의 요구에 따라 네일 폴리시 색상의 질감을 학기 위한 베이스코트를 아주 얇게 도포할 수 있다.			
	작업 매뉴얼에 따라 네일 폴리시를 얼룩 없이 균일하게 도포할 수 있다.			
	작업 매뉴얼에 따라 네일 폴리시 도포 후 컬러 보호와 광택 부여를 위한 톱코트를 바를 수 있다.			

## 피드백은

평가 후에 학습자들에게 평가 결과를 피드백하여 부족한 부분을 알려주고, 학습 결과가 미진한 경우, 해당 부분을 다시 학습하여 학습목표를 달성하는 데 활용할 수 있습니다.

## 피드백

1. 작업장 평가
  - 작업 결과물을 확인하여 수정사항을 제시하고 수정 부분을 인지하도록 한다.

## 4. 참고 자료

## 참고자료

## 참고자료는

해당 학습모듈의 필요지식에 대한 출처와 인용한 참고 자료 및 사이트를 제시하였습니다.

- 김미원(2011). 『Nail Study』. 서울: 사)한국네일저서서비스협회.
- 민방경(2015). 『비용·사(네일)평가』. 서울: 예문사.
- 박은주(2014). 『네일비용』. 서울: 정담미디어.

## 5. 활용 서식/부록


## 활용서식

## 활용서식은

평가 서식, 실습시트 등 교수학습 시 활용 가능한 다양한 서식들로 구성하였습니다. 과제 진행에서 평가에 이르기까지 필요한 서식을 해당 학습모듈의 특성에 맞춰 개발하거나 기존의 양식을 활용하여 제시하였습니다.

## 프리에지 형태 실습지

1. 프리에지 형태의 이해

모 양	이름	특 징
	이름 ( Square nail )	특 징 - 강한 느낌의 사각형태 - 네일의 양끝 모서리 부분이 90° 사각의 형태이다. ( ) - 발톱의 형태 활용 - 내인성 발톱의 보정사에 적용

## 부록은

활용서식 이외에 교수학습과정에서 참고할 수 있는 자료가 있는 경우 제시하였습니다.

## 부록

## 네일 기본관리 도구와 재료 목록

목록	비고	준비
위생가운	흰색	작업자 착용
위생 마스크	흰색	작업자 착용
보호안경	투명한 렌즈 (안경으로 대체 가능)	작업자 착용
재용정리함	재질, 색상 무관	작업대

# [NCS-학습מוד의 위치]

대분류	정보 통신	
중분류	정보 기술	
소분류	정보 기술 개발	

세분류	능력단위	학습מוד명
SW아키텍처	보안계획 수립	보안계획 수립
응용SW 엔지니어링	보안위협 평가	보안위협 평가
임베디드SW 엔지니어링	보안요구사항 정의	보안요구사항 정의
DB엔지니어링	관리적 보안 구축	관리적 보안 구축
NW엔지니어링	물리적 보안 구축	물리적 보안 구축
보안엔지니어링	소프트웨어 개발 보안 구축	소프트웨어 개발 보안 구축
UI/UX엔지니어링	데이터베이스 보안 구축	데이터베이스 보안 구축
시스템SW 엔지니어링	시스템 보안 구축	시스템 보안 구축
빅데이터 플랫폼구축	네트워크 보안 구축	네트워크 보안 구축
핀테크 엔지니어링	보안체계 운영관리	보안체계 운영관리
데이터아키텍트	보안위협 관리통제	보안위협 관리통제
	보안감사 수행	보안감사 수행
	보안인증 관리	보안인증 관리

---

# 차 례

---

학습모듈의 개요 .....	1
<b>학습 1. 네트워크 보안 설계하기</b>	
1-1. NW보안 요구사항명세 .....	3
1-2. NW보안 설계 .....	32
1-3. NW구현 준비 .....	47
• 교수·학습 방법 .....	51
• 평가 .....	52
<b>학습 2. 네트워크 보안 구현하기</b>	
2-1. NW보안 구현 .....	54
2-2. NW보안 테스트 .....	63
• 교수·학습 방법 .....	69
• 평가 .....	70
참고 자료 .....	72



# 네트워크 보안 구축 학습모듈의 개요

## 학습모듈의 목표

정의된 보안요구사항에 따라 네트워크 보안 요구사항을 명세하고 설계, 구현, 테스트할 수 있다.

## 선수학습

보안위협관리통제(2001020603\_16v3), 네트워크보안관리(LM2002010310\_14v2), 근거리통신망(LAN) 설계(LM2002010312\_16v1), L2 • L3 스위치 구축(LM2002010313\_16v1), 무선랜 구축(LM2002010314\_16v1)

## 학습모듈의 내용체계

학습	학습 내용	NCS 능력단위 요소	
		코드번호	요소 명칭
1. 네트워크 보안 설계하기	1-1. NW보안 요구사항명세	2001020614_16v3.1	네트워크 보안 설계하기
	1-2. NW보안 설계		
	1-3. NW구현 준비		
2. 네트워크 보안 구현하기	2-1. NW보안 구현	2001020614_16v3.2	네트워크 보안 구현하기
	2-2. NW보안 테스트		

## 핵심 용어

네트워크 보안, DDoS, 방화벽, IDS, IPS, 웹방화벽, 악성코드, 망분리, NAC, 보안 관제





# 학습 1 네트워크 보안 설계하기

## 학습 2 네트워크 보안 구현하기

### 1-1. NW보안 요구사항명세

**학습 목표** • 정의된 보안요구사항에 따라 네트워크에 대한 보안 요구사항을 명세할 수 있다.

#### 필요 지식 /

##### ① 네트워크 보안 설계를 위한 고려사항

기본적으로 네트워크 보안 설계는 기관의 서버 및 클라이언트 네트워크의 내외부에서 유발되는 사이버 침해 공격으로 인한 보안 리스크를 최소화하기 위한 것이다. 이를 위하여 다양한 네트워크 보안 설계 요구사항이 존재하며, 특히 개인정보의 유출을 방지하기 위한 법률 요건이 존재하므로 법률 규제사항의 구조에 대한 이해가 필요하다.

##### 1. 개인정보 보호와 관련된 법률

개인정보 보호와 관련되어 특별법과 일반법이 존재한다.

###### (1) 특별법

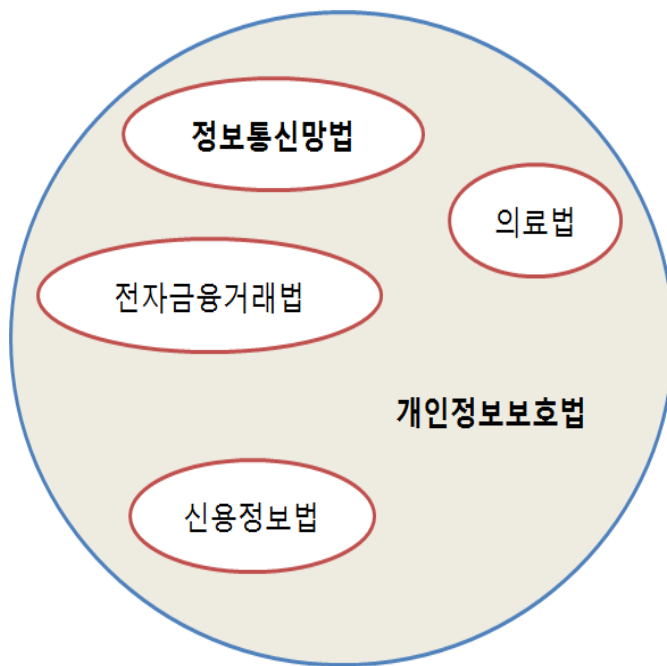
정보통신분야의 정보통신망법이나 의료분야의 환자정보 처리 등에 대한 의료법, 금융 분야에 적용되는 전자금융거래법 등과 같이 사업 분야별로 적용되는 법이다.

###### (2) 일반법

개인정보 보호법과 같이 특별법에서 정의하지 않는 잔여 영역에 대해 포괄적으로 적용되는 법이다.

###### (3) 특별법과 일반법의 관계

특별법이 일반법과 충돌할 경우 특별법이 우선 적용된다. 특별법에서 정의하지 않는 잔여 영역에 대해서는 일반법이 적용된다.



[그림 1-1] 각종 특별법과 일반법인 개인정보 보호법의 관계

<표 1-1> 의료법을 예시로 든 특별법과 일반법의 관계

구분	진료 정보	일반 개인정보
개념	진료를 목적으로 수집하여 처리하는 개인정보 가 포함된 정보 - 진료기록부, 수술기록부, 조산기록부, 간호 기록부, 환자명부 등	홈페이지 회원정보, 홍보를 위한 연 락처 등 일반 개인정보
일반원칙	의료법에 규정이 있는 경우 의료법을 우선 적용 - 규정이 없는 경우 개인정보 보호법 적용	개인정보 보호법을 적용
수집이용	의료법 제22조(시행규칙 제14조) - 동의 없이 수집 가능 - 진료 목적으로만 사용 가능	개인정보 보호법 제15조 - 동의를 받아 수집
관리	개인정보 보호법 - 제26조: 문서로 위탁해야 하며 위탁 사실을 공개해야 함 - 제29조: 안전한 관리를 위해 접근통제, 암호화, 접속기록 보관, 물리적 보호조치 등 안전성 확보조치를 해야 함 - 제30조: 개인정보처리 방침을 수립하여 공개해야 함 - 제31조: 개인정보보호 책임자를 지정해야 함	

## 2. 네트워크 보안 관련 법률 규제 구성

규제 기준으로써 참조해야 하는 법은 법률과 시행령, 시행규칙 등으로 구성된다.

### (1) 정보통신망법 관련 규제 구성

정보통신망법은 정보통신망을 통해 서비스를 제공하는 사업자를 대상으로 하는 법률로써, 일반적으로 개인정보보호 규제의 대표적 법률이라고 할 수 있다.

#### (가) 정보통신망법

정보통신망의 이용 촉진에 대한 내용과 정보보호 규제에 대한 내용 위법 시 벌칙에 대한 내용이 포함되어 있다.

#### (나) 정보통신망법 시행령

정보통신망법의 하위 기준으로써 개인정보의 보호조치를 위해 대통령령으로 제정된 시행령이다.

#### (다) 개인정보의 기술적 관리적 보호조치 기준

정보통신망법 시행령의 하위 기준으로써, 방송통신위원회가 시행령 제1항부터 제5항까지의 규정에 따른 사항과 법 제28조제1항, 제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시한 것이다.

#### (라) 정보보호관리체계 인증 기준

정보통신망법 제47조에 근거하여 제47조 2항에서 정의하는 기준에 해당하는 사업자는 의무적으로 정보보호관리체계 인증을 받아야 하며, 이 인증에 대한 세부 심사 기준 항목이 존재한다.

### (2) 개인정보 보호법 관련 규제 구성

개인정보 보호법은 특별법에 적용되지 않는 영역에 적용되는 일반법이다.

#### (가) 개인정보 보호법

개인정보 보호법은 개인정보의 처리 및 보호에 관한 사항 및 이에 대한 위법 시의 벌칙 기준에 대한 내용이 포함되어 있다.

#### (나) 개인정보 보호법 시행령

개인정보 보호법의 하위 기준으로써 개인정보의 보호조치를 위해 대통령령으로 제정된 시행령이다.

#### (다) 개인정보의 안전성 확보조치 기준

개인정보 보호법 시행령의 하위 기준으로써, 행정안전부장관이 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시한 것이다.

#### (라) 개인정보보호관리체계 인증 기준

개인정보 보호법 제32조2항에 근거하며, 개인정보 보호를 위한 정책 수립, 개인정보의 수명주기관리, 개인정보 보호대책의 적절한 적용을 준수하는지 인증하는 것으로써, 이 인증에 대한 세부 심사기준 항목이 존재하며 의무 인증은 아니다.

## ② 네트워크 침해 공격과 관련된 주요 용어 개념

네트워크 보안설계를 위해 사이버 공격 및 대응 관련 기본 용어의 이해가 필요하다.

### 1. 사이버 공격 관련 주요 용어의 개념

사이버 침해 공격에 활용되는 기법에 대한 주요 용어는 다음과 같다.

<표 1-2> 정보보안 침해 공격 방법 관련 기본 용어

용어	의미
디도스(DDoS) 공격	다수의 악성 코드 감염PC를 이용해 대규모 트래픽을 특정 시스템에 전송하여 네트워크 및 시스템의 과부하를 일으키고 정상 서비스를 방해하는 사이버 침해 공격
스미싱	스마트폰 문자 발송 메시지를 통해 악성 앱 설치를 유도하고 개인정보 혹은 금융 정보를 탈취하는 침해 기법
스피어 피싱	창(Spear)와 피싱(Phishing)의 합성어로 특정 공격 대상을 지정하고 다양한 방법을 통해 집중적으로 공격 대상을 공격하여 정보를 탈취하기 위한 수법
웹 해킹	웹 서비스 요소를 공격하여 이용자 혹은 관리자의 권한을 획득하고 개인정보 등을 탈취하는 행위
지능형 지속공격 (APT, Advanced Persistent Threat)	특정 대상에 대해 명확한 목표를 설정하고 지능적이고 지속적으로 공격을 가하여 정보를 수집 및 유출하는 해킹기법
포트 스캐닝	공격 대상 서버의 열린 서비스 포트를 순차적으로 접속 시도함으로써, 취약한 포트를 찾아내는 공격 준비 기법
무작위 대입공격	Brute-force 공격이라고도 부르며, 사용자 인증이 필요한 기능에 비밀번호 등을 무작위로 대입하여 인증 성공을 노리는 공격 기법
미라이봇넷	IoT 기기를 통해, DDos 공격을 하는 봇넷의 일종으로써 IoT 기기의 기본 계정을 통해 통제권을 획득하거나 다량의 트래픽을 유발하는 공격 방법



## 2. 정보 보안 침해 공격에 사용되는 프로그램 관련 주요 용어

정보 보안 침해 공격에 사용되는 악성 프로그램 관련 주요 용어는 다음과 같다.

<표 1-3> 정보 보안 침해 공격에 사용되는 악성 프로그램 관련 기본 용어

용어	의미
랜섬웨어	사용자 컴퓨터나 서버 시스템에 동의없이 설치되어 파일을 암호화하고, 복호화를 원하는 사용자에게 돈을 요구하는 사이버 범죄에 사용되는 악성 프로그램
루트킷	해커에 의해 설치된 악성코드가 백신이나 사용자에게 감지되지 않도록 숨겨주는 악성 프로그램
C&C 서버	해커에 의해 악성코드에 감염된 좀비 PC를 관리하고 DDoS와 같은 공격 명령을 내리는 관리 및 제어 목적의 서버
컴퓨터 바이러스	정상적인 실행 파일과 결합하여 PC의 동작을 중지시키거나 파일을 변조 혹은 파괴하는 등 컴퓨터의 운영을 방해하는 악성 프로그램
백도어	사용자 컴퓨터나 서버 시스템에 해커가 사용자 몰래 접속하여 악의적인 행위를 할 수 있도록 출입구 역할을 해주는 악성 프로그램
좀비 PC	해커가 원격에서 제어할 수 있는 악성 프로그램이 설치되어, 사용자 모르게 스팸 발송, 악성코드 유포, DDoS 등의 공격에 활용되는 컴퓨터
웜(worm)	다른 파일을 변조하여 기생하지 않고 독자적으로 자신을 복제하여 확산함으로써 전파 속도가 매우 빠른 특징을 지니며 주로 메일, 네트워크 공유 폴더 등을 통해 전파되고 시스템과 네트워크에 부하를 증가시키는 악성 프로그램
웹셀	해커가 원격으로 웹서버 시스템에 악의적인 명령을 실행할 수 있도록 작성한 웹 브라우저 기반의 스크립트 실행 파일
익스플로잇 (Exploit)	해커가 소프트웨어나 하드웨어의 취약점을 통해 악성 행위를 수행하기 위해 제작한 프로그램
제로데이 취약점	보안 패치가 발표되지 않은 상태에서 외부에 노출된 취약점
키로거	사용자의 키보드 입력 데이터를 해커에게 전송하는 악성 프로그램
트로이 목마	컴퓨터에 숨어 있으면서 사용자의 정보를 사용자가 인지하지 못하도록 유출하는 악성코드

### 3. 주요 웹 해킹 공격 유형

사이버 침해 공격 중 웹 해킹과 관련된 주요 유형은 다음과 같다.

<표 1-4> 정보보안 침해 공격 방법 관련 기본 용어

용어	의미
SQL 인젝션	SQL을 사용하는 응용 프로그램에서 SQL구문을 조작하여 인증 우회 혹은 권한 상승을 유발하는 공격
크로스 사이트 스크립트(XSS, Cross Site Script)	웹사이트에 악성 스크립트를 삽입할 수 있는 취약점을 활용하여, 의도하지 않은 기능을 수행하거나 중요 정보를 탈취하는 공격
크로스 사이트 요청 위조(CSRF, Cross Site Request Forgery)	웹서버가 피해자의 정당한 웹 요청이라고 오해하게 만들도록 웹사이트에 피해자의 세션 쿠키 및 인증정보를 자동으로 포함하여 위조된 웹 요청을 강제로 보내도록 하는 공격
파일 업로드(웹쉘)	허용되지 않은 유형의 파일을 업로드하고 해당파일을 외부에서 직접 접근할 수 있는 취약점을 활용하여 웹서버를 쉘을 탈취하는 공격
파일 다운로드	검증되지 않은 외부 입력값을 이용하여 서버의 파일에 접근하고 식별 가능한 취약점을 이용하여 중요 서버 파일을 탈취하는 공격
세션 탈취	크로스 사이트 스크립트 등의 방법을 이용하여 피해자의 세션 쿠키를 탈취하고 이를 이용해 피해자의 세션으로 로그인하는 공격

## 수행 내용 / NW보안 요구사항명세하기

### 재료 · 자료

- 정보통신망 이용촉진 및 정보보호 등에 관한 법률
- 개인정보 보호법
- 정보보호관리체계에 관한 국제 표준 규격(ISO27001)
- 정보보호관리체계(ISMS) 인증 기준 세부 점검항목
- 개인정보보호관리체계(PIMS) 인증 기준 세부 점검항목

### 기기(장비 · 공구)

- 인터넷
- 컴퓨터
- 프린터
- 문서 작성 도구

### 안전 · 유의 사항

- 네트워크 보안 설계 요구사항 도출을 위해 각종 규제 기준을 확인한다.
- 정보통신망법과 개인정보 보호법을 기반으로 세부 가이드를 확인한다.
- 정보보호관리체계 인증 기준과 개인정보보호관리체계 인증 기준을 확인한다.

### 수행 순서

#### ① 정보보안과 관련된 국내 규제 및 가이드 기준을 확인한다.

네트워크 보안과 관련되어 반드시 준수가 필요한 국내 법규 기준을 확인한다.

##### 1. 정보통신망법상의 네트워크 보안 관련 기준을 확인한다.

국내 정보보호관련 법률의 근간이 되는 정보통신망법 중 네트워크 보안과 관련된 기준을 확인한다.

##### (1) 국가법령정보센터에 접속하여 정보통신망법의 네트워크 보안관련 기준을 확인한다.

국내 모든 법률을 검색할 수 있는 국가법령정보센터에 접속하여 정보통신망 이용촉진 및 정보보호 등에 관한 법률을 검색하고 네트워크 보안 관련 기준을 확인한다.

(가) 국가법령정보센터에 접속한다.

법제처에서 운영하는 국가법령정보센터(<http://www.law.go.kr>)에 접속한다.



출처: 국가법령정보센터(<http://www.law.go.kr>) 2018.5.31. 스크린샷

[그림 1-2] 국가법령정보센터 접속 화면

(나) 정보통신망 이용촉진 및 정보보호 등에 관한 법률 및 시행령을 검색한다.

검색창에 ‘정보통신망’을 입력하고 검색을 클릭하여 정보통신망법 및 시행령을 검색한다.



출처: 국가법령정보센터(<http://www.law.go.kr>) 2018.5.31. 스크린샷

[그림 1-3] 정보통신망법 및 시행령 검색 화면

(다) 정보통신망법을 클릭하여 네트워크 보안 관련 기준을 확인한다.

정보통신망법 제28조(개인정보의 보호조치)와 제47조(정보보호 관리체계의 인증) 기준의 내용을 확인한다.

1) 정보통신망법 제28조(개인정보의 보호조치) 내용을 확인한다.

법의 내용 중 침입차단시스템 중 접근 통제 장치의 설치 및 운영이 필요함을 확인한다.

#### 정보통신망 이용촉진 및 정보보호 등에 관한 법률

##### 제28조(개인정보의 보호조치)

① 정보통신서비스 제공자 등이 개인정보를 처리할 때에는 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성을 확보하기 위하여 대통령령으로 정하는 기준에 따라 다음 각 호의 기술적·관리적 조치를 하여야 한다.

1. 개인정보를 안전하게 처리하기 위한 내부관리계획의 수립·시행

2. 개인정보에 대한 불법적인 접근을 차단하기 위한 침입차단시스템 등 접근 통제 장치의 설치·운영

..(중략)..

2) 정보통신망법 제47조(개인정보의 보호조치) 내용을 확인한다.

법의 내용 중 ISP와 같은 정보통신망 제공 사업자, IDC사업자와 같은 집적정보통신설비 제공업자, 그리고 일정한 규모 이상의 정보통신망 기반 서비스제공업자는 ISMS 인증 의무 대상자임을 확인한다.

#### 정보통신망 이용촉진 및 정보보호 등에 관한 법률

##### 제47조(정보보호 관리체계의 인증)

..(중략)..

② 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자로서 다음 각 호의 어느 하나에 해당하는 자는 제1항에 따른 인증을 받아야 한다.

1. 「전기통신사업법」 제6조제1항에 따른 허가를 받은 자로서 대통령령으로 정하는 바에 따라 정보통신망서비스를 제공하는 자

2. 집적정보통신시설 사업자

3. 연간 매출액 또는 세입 등이 1,500억원 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상 또는 3개월간의 일일평균 이용자수 100만명 이상으로서, 대통령령으로 정하는 기준에 해당하는 자



(라) 정보통신망법 시행령을 클릭하여 네트워크 보안 관련 기준을 확인한다.

정보통신망법 시행령 제15조(개인정보의 보호조치) 기준의 내용을 확인한다.

1) 정보통신망법 시행령 제15조(개인정보의 보호조치) 내용을 확인한다.

시행령 2항을 통해 침입차단시스템 및 침입탐지시스템의 설치 운영에 관한 기준과, 개인정보 취급자 컴퓨터에 대한 외부 인터넷 망 차단(망분리)에 대한 기준을 확인한다. 시행령 6항을 통해 방송통신위원회가 고시하도록 되어있는 개인정보의 안전성 확보를 위해 필요한 보호조치에 대한 고시 기준을 별도로 조사해야 함을 확인한다.

#### 정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령

##### 제15조(개인정보의 보호조치)

② 법 제28조제1항제2호에 따라 정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위하여 다음 각 호의 조치를 하여야 한다.  
..(중략)..

2. 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영

3. 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷 망 차단  
..(중략)..

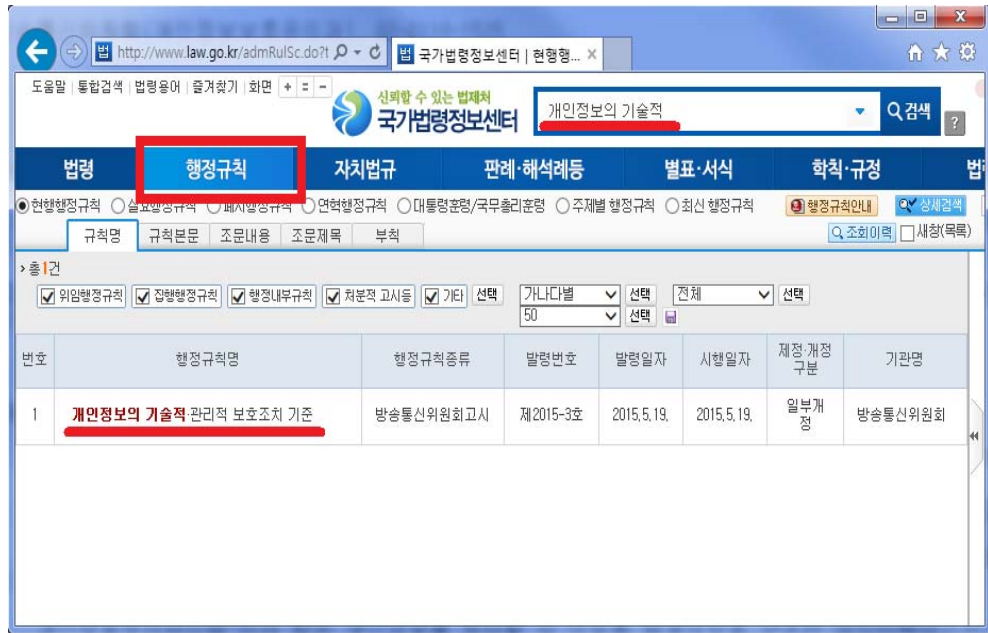
⑥ 방송통신위원회는 제1항부터 제5항까지의 규정에 따른 사항과 법 제28조제1항 제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다.

(2) 정보통신망법과 연관된 개인정보의 기술적 관리적 보호조치 기준의 네트워크 보안 관련 내용을 확인한다.

국가법령정보센터에서 개인정보의 기술적 관리적 보호조치 기준을 검색하고 네트워크 보안 관련 기준을 확인한다.

(가) 개인정보의 기술적 관리적 보호조치 기준을 검색한다.

국가법령정보센터 웹사이트에서 상단의 행정규칙 분야를 선택하고 ‘개인정보의 기술적 관리적 보호조치 기준’을 검색한다.



출처: 국가법령정보센터(<http://www.law.go.kr/>) 2018.5.31. 스크린샷  
[그림 1-4] 개인정보의 기술적 관리적 보호조치 기준 검색 화면

(나) 개인정보의 기술적 관리적 보호조치 기준을 클릭하여 네트워크 보안 관련 기준을 확인한다.

개인정보의 기술적 관리적 보호조치 기준 제4조(접근통제)의 내용을 통해 IP 접근통제를 위한 방화벽, 불법적인 개인정보 유출 탐지를 위한 IDS의 장비가 필요함을 확인한다. 또 개인정보를 다운로드 혹은 파기할 수 있거나 개인정보처리시스템에 대한 접근 권한을 설정할 수 있는 개인정보 취급자의 컴퓨터에 대한 망분리가 필요함을 확인한다.

### 개인정보의 기술적·관리적 보호조치 기준

#### 제4조(접근통제)

⑤ 정보통신서비스 제공자 등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 허가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

⑥ 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자 등은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하여야 한다.

## 2. 개인정보 보호법 상의 네트워크 보안 관련 기준을 확인한다.

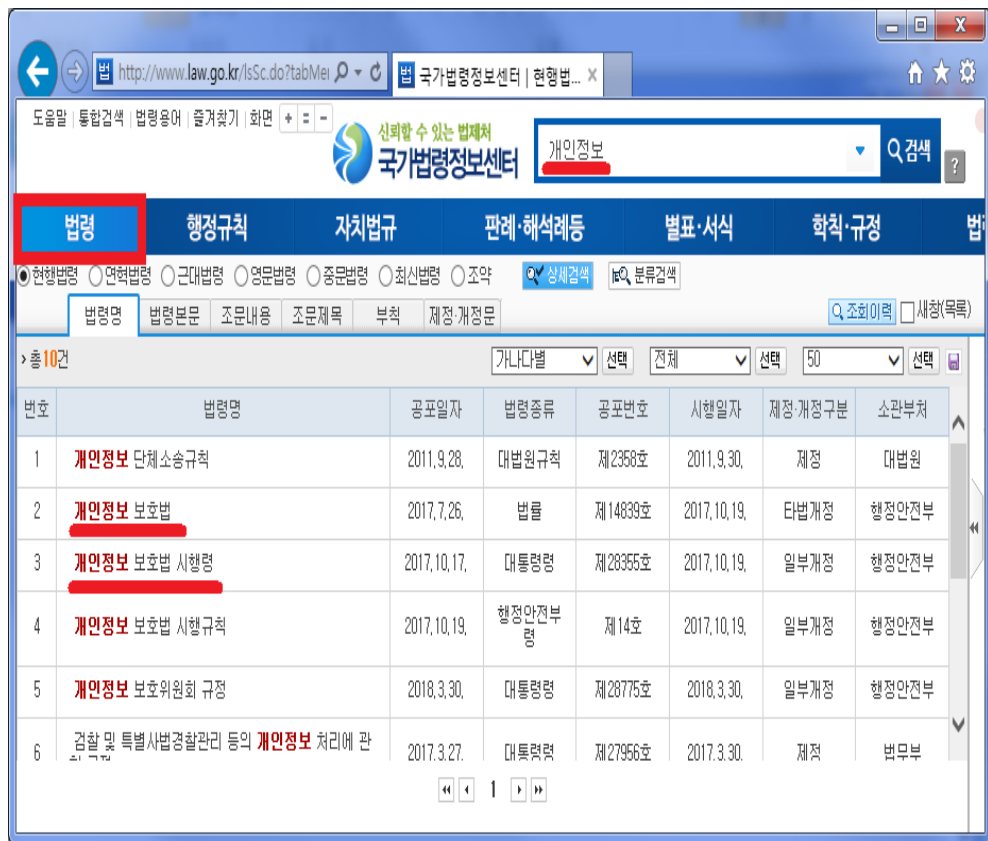
국내 정보보호 관련 일반법 역할을 수행하는 개인정보 보호법 중 네트워크 보안과 관련된 기준을 확인한다.

(1) 국가법령정보센터 웹사이트를 통해 개인정보 보호법의 네트워크 보안 관련 기준을 확인한다.

국가법령정보센터 웹사이트를 통해 개인정보 보호법을 검색하고 네트워크 보안 관련 기준을 확인한다.

(가) 국가법령정보센터에서 개인정보 보호법 및 시행령을 검색한다.

국가법령정보센터 검색창에 ‘개인정보’를 입력하고 검색을 클릭하여 개인정보 보호법 및 시행령을 검색한다.



출처: 국가법령정보센터(<http://www.law.go.kr/>) 2018.5.31. 스크린샷  
[그림 1-5] 개인정보 보호법 및 시행령 검색 화면

(나) 개인정보 보호법을 클릭하여 네트워크 보안 관련 기준을 확인한다.

개인정보 보호법 제29조(안전조치의무)와 제32조의2(개인정보 보호 인증) 기준의 내용을 확인한다.

1) 개인정보 보호법 제29조(안전조치의무) 내용을 확인한다.

법의 내용 중 기술적 관리적 조치가 필요함을 확인한다.

#### 개인정보 보호법

##### 제29조(안전조치의무)

개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

2) 개인정보 보호법 제32조의2(개인정보 보호 인증) 내용을 확인한다.

법의 내용 중 개인정보 처리 사업자가 PIMS 인증을 의무가 아닌 선택사항으로 받을 수 있음을 확인한다.

#### 개인정보 보호법

##### 제32조의2(개인정보 보호 인증)

① 행정안전부장관은 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 이 법에 부합하는지 등에 관하여 인증할 수 있다.

...(중략)...

(다) 개인정보 보호법 시행령을 클릭하여 네트워크 보안 관련 기준을 확인한다.

개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치) 기준의 내용을 확인한다.

1) 개인정보 보호법 시행령 제30조(개인정보의 안전성 확보 조치) 내용을 확인한다.

시행령 1항을 통해 개인정보 처리시스템에 대한 접근 통제 필요성을 확인한다.

시행령 3항을 통해 행정안전부 장관이 고시하도록 되어있는 개인정보의 안전성 확보 조치에 관한 세부 고시 기준을 별도로 조사해야 함을 확인한다.

#### 개인정보 보호법 시행령

##### 제30조(개인정보의 안전성 확보 조치)

① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.

1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행

2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치

...(중략)...

③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 행정안전부장관이 정하여 고시한다.

(2) 개인정보 보호법과 연관된 개인정보의 안전성 확보 조치 기준의 네트워크 보안 관련 내용을 확인한다.

국가법령정보센터에서 개인정보의 안전성 확보 조치 기준을 검색하고 네트워크 보안 관련 기준을 확인한다.

(가) 개인정보의 안전성 확보 조치 기준을 검색한다.

국가법령정보센터 웹사이트에서 상단의 행정규칙 분야를 선택하고 ‘개인정보의 안전성 확보 조치 기준’을 검색한다.



출처: 국가법령정보센터(<http://www.law.go.kr/>) 2018.5.31. 스크린샷

[그림 1-6] 개인정보의 안전성 확보조치 기준 검색 화면

(나) 개인정보의 안전성 확보조치 기준을 클릭하여 네트워크 보안 관련 기준을 확인한다.

개인정보의 안전성 확보조치 기준 제6조(접근통제)의 내용을 통해 IP접근통제를 위한 방화벽, 불법적인 개인정보 유출 탐지를 위한 IDS의 장비가 필요함을 확인한다. 또 외부에서 정보통신망을 통해 개인정보처리시스템에 접속하는 경우를 위한 VPN의 구축이 필요함을 확인한다.

### 개인정보의 안전성 확보조치 기준

#### 제6조(접근통제)

① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 허가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응

② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

...(중략)...



### 3. ISMS 인증 기준 상의 네트워크 보안 관련 기준을 확인한다.

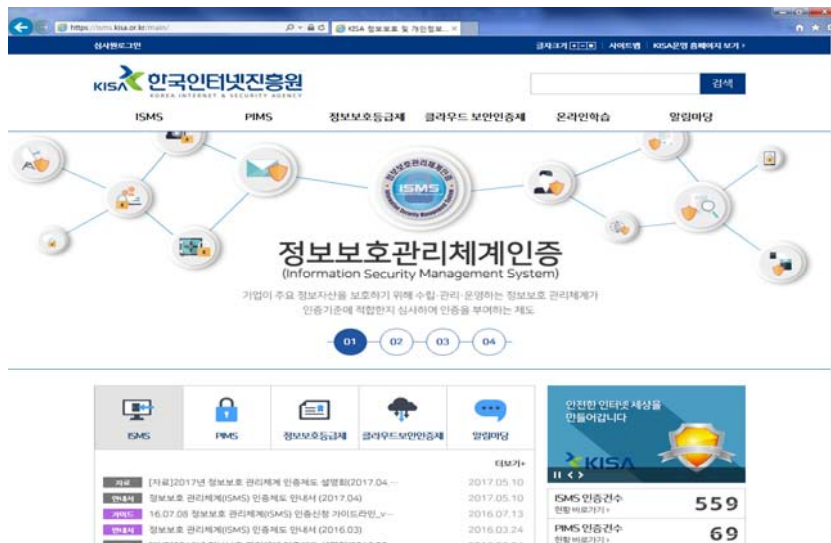
정보통신망법 제47조2항에 따른 ISMS인증과 관련하여 인증 기준상의 네트워크 보안과 관련된 기준을 확인한다.

#### (1) 한국인터넷진흥원 웹사이트를 통해 ISMS인증기준의 네트워크 보안 관련 기준을 확인한다.

한국인터넷진흥원의 ISMS 지원 웹사이트를 통해 ISMS인증기준을 검색하고 네트워크 보안 관련 기준을 확인한다.

##### (가) ISMS지원 웹사이트에 접속한다.

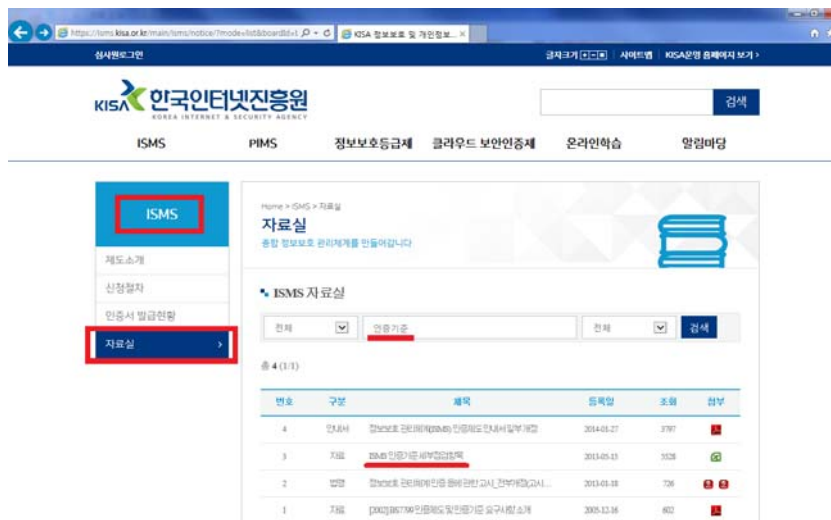
한국인터넷진흥원에서 운영하는 ISMS지원 웹사이트(<http://isms.kisa.or.kr>)에 접속한다.



출처: 인터넷진흥원(<http://isms.kisa.or.kr>) 2018.5.31. 스크린샷  
[그림 1-7] ISMS지원 웹사이트 접속화면

##### (나) ISMS 인증 기준을 검색한다.

ISMS 자료실 검색창에 '인증기준'을 입력하고 검색을 클릭하여 ISMS 인증기준을 다운로드한다.



출처: 인터넷진흥원(<http://isms.kisa.or.kr>) 2018.5.31. 스크린샷  
[그림 1-8] ISMS 인증기준 세부 점검항목

(다) ISMS 인증기준 세부 점검항목 중 네트워크 보안 관련 기준을 확인한다.

ISMS 인증기준 세부 점검항목 중 10. 접근통제와 11. 운영보안의 분야에서 네트워크 보안 관련 내용을 확인한다.

1) ISMS 인증기준 세부 점검항목 중 10. 접근통제 분야에서 네트워크 보안 관련 내용을 확인한다.

네트워크에 대한 비인가 접근을 통제하기 위한 접근통제 리스트, IP 등 식별자에 대한 관리체계를 수립하고, 내/외부 네트워크를 분리해야 함을 확인한다.

<표 1-5> ISMS 인증기준 세부 점검 항목 중 10. 접근통제 - 관리 기준

통제항목	목적	점검 항목	설명
네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위해 필요한 네트워크 접근 통제리스트, 네트워크 식별자 등에 대한 관리절차를 수립하고 서비스, 사용자 그룹, 정보자산의 중요도에 따라 내·외부 네트워크를 분리하여야 한다.	접근통제 정책에 따라 인가된 사용자만이 네트워크에 접근할 수 있도록 네트워크 식별자(IP) 할당 등을 통제하고 있는가?	<ul style="list-style-type: none"> <li>정보시스템, PC 등에 IP를 부여하는 경우 승인 절차에 따라 부여하고 허가되지 않은 IP의 사용은 통제하여야 하며 인가된 사용자/단말만이 네트워크에 접근할 수 있도록 하여야 한다.</li> <li>특별히 업무를 위하여 필요하지 않은 경우 네트워크 장비에 설치된 포트, 서비스를 제거 또는 차단하여야 한다.</li> </ul>
		네트워크 구성 변경 시에는 공식적인 변경 관리 절차를 준수하고 자체적인 보안성 검토를 수행하고 있는가?	네트워크 신규 생성 및 변경은 조직의 정보보호 환경에 많은 영향을 미치기 때문에 주요 변경에 대해서는 보안성을 검토하고 책임자의 승인을 받아야 한다.
		네트워크를 구성하는 주요자산 목록, 구성도, IP 현황을 최신으로 유지하고 안전하게 관리하고 있는가?	<ul style="list-style-type: none"> <li>네트워크를 구성하는 주요자산 목록, 구성도, IP 현황 등을 최신으로 유지하고 외부에 유출되지 않도록 대외비 이상으로 안전하게 관리하여야 한다.</li> <li>- 최소한의 인력만 접근, 전자 문서 형태로 관리할 경우 암호 설정 등</li> </ul>

출처: ISMS 인증기준 세부 점검항목

<표 1-6> ISMS 인증 기준 세부 점검 항목 중 10. 접근통제 - 네트워크 분리

통제항목	목적	점검 항목	설명
네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위해 필요한 네트워크 접근 통제리스트, 네트워크 식별자 등에 대한 관리절차를 수립하고 서비스, 사용자 그룹, 정보자산의 중요도에 따라 내·외부 네트워크를 분리하여야 한다.	내부 네트워크 IP 주소는 사실 IP로 할당하고 국제권고표준을 따르고 있는가?	<ul style="list-style-type: none"> <li>• 내부망에서의 주소 체계는 사실 IP주소 체계를 사용하고 내부 주소체계를 외부에 유출되지 않도록 하여야 하며 외부 네트워크와의 연결지점에 NAT (Network Address Translation) 기능을 적용하여야 한다.</li> <li>• 사실 IP주소를 할당하는 경우 국제표준에 따른 사실 IP주소대역을 사용하여야 한다.</li> </ul> <p>※ 사실 IP주소대역 ※</p> <ul style="list-style-type: none"> <li>- 10.0.0.0 ~ 10.255.255.255</li> <li>- 172.16.0.0 ~ 172.31.255.255</li> <li>- 192.168.0.0 ~ 192.168.255.255)</li> </ul>
		서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항에 따라 네트워크 영역을 물리적 또는 논리적으로 분리하고 있는가?	<ul style="list-style-type: none"> <li>• 핵심 업무영역의 네트워크는 위험평가를 통해 물리적 또는 논리적으로 영역을 분리하고 영역 간 접근을 통제하여야 한다.</li> <li>- (DMZ) 외부로부터의 접근이 불가피한 웹 서버, 메일서버 등의 공개용 서버는 DMZ 영역에 위치시키고 공개서버를 경유하여 내부 업무망으로의 접근이 이루어지지 않도록 접근통제를 수행하여야 한다.</li> <li>- (서버팜) 서버들이 위치하는 영역(서버 팜)은 다른 네트워크 영역과 구분되고 인가 받은 내부사용자의 접근만을 허용하도록 접근통제 정책을 적용하여야 한다.</li> <li>- (DB팜) 조직의 중요정보가 저장된 DB가 위치한 네트워크 영역은 다른 네트워크 영역과 분리하여야 한다.</li> <li>- (운영환경) 서버, 보안장비, 네트워크장비 등을 운영하는 인력이 사용하는 네트워크 영역은 별도로 분리하여야 한다.</li> <li>- (개발환경) 개발업무(개발자PC, 개발서버, 테스트서버 등)에 사용되는 네트워크는 별도 망으로 구성하여 운영에 사용되는 네트워크와 분리하여야 한다.</li> <li>- (외부자) 외부 사용자에게 서비스를 제공하는 네트워크(외주용역, 민원실, 교육장 등)는 내부 업무용 네트워크와 분리하여야 한다.</li> <li>- (기타) 업무망의 경우 업무의 특성, 중요도에 따라 네트워크 대역 분리기준을 수립하여 운영하여야 한다.</li> </ul> <p>※ 다만 기업의 규모 등을 고려하여 서버 팜/DB팜을 세부적으로 분리하기 어려운 경우 추가적인 보완대책을 마련하여야 한다. (호스트 기반 접근통제 등)</p>

출처: ISMS 인증기준 세부 점검항목

<표 1-7> ISMS 인증 기준 세부 점검 항목 중 10. 접근통제 - 네트워크 간 연동

통제항목	목적	점검 항목	설명
네트워크 접근	네트워크에 대한 비인가 접근을 통제하기 위해 필요한 네트워크 접근통제 리스트, 네트워크 식별자 등에 대한 관리절차를 수립하고 서비스, 사용자 그룹, 정보자산의 중요도에 따라 내·외부 네트워크를 분리하여야 한다.	접근통제 정책에 따라 분리된 네트워크 영역 간에 침입차단시스템 등을 통한 접근통제를 하고 있는가?	<ul style="list-style-type: none"> <li>• 침입차단시스템, ACL(Access Control List) 설정이 가능한 네트워크 장비 등을 활용하여 네트워크 영역 간 업무수행에 필요한 서비스의 접근만 허용하도록 통제하여야 한다.</li> <li>- 특히 외부(인터넷)로부터의 불법적인 접근 및 침해시도를 방지하기 위해 침입차단 시스템 등을 통하여 내부 네트워크 접근은 더욱 엄격하게 통제하여야 한다.</li> </ul>
		물리적으로 떨어진 IDC 센터, 지사, 대리점 등과의 네트워크 연결 시 전용 회선을 구축하고 전용선 구축이 불가능한 경우 VPN(가상사설망) 등의 대책을 마련하고 있는가?	물리적으로 떨어진 장소와 네트워크 연결이 필요한 경우 전용회선 또는 VPN을 활용하여 보안성을 강화하여야 한다.

출처: ISMS 인증기준 세부 점검항목

2) ISMS 인증기준 세부 점검항목 중 11. 운영보안 분야에서 네트워크 보안 관련 내용을 확인한다.

보안 시스템 운영에 대한 관리절차 수립 및 접근통제, 적용 정책의 현행화 관리 필요성에 대한 내용을 확인한다. 시스템을 사내망에서 원격 운영하는 경우 관리자 PC에 대한 IP/MAC 접근제어를 수행해야 하고, 외부망에서의 원격 접속 운영은 원칙적으로 금지하되 부득이한 경우 준수해야 할 관리기준에 대해 확인한다. 무선랜 등의 무선네트워크 보안에 대한 기술적 관리적 기준을 확인한다.

<표 1-8> ISMS 인증기준 세부 점검 항목 중 11. 운영보안 - 보안시스템 운영

통제항목	목적	점검 항목	설명
보안 시스템 운영	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영 절차를 수립하고 보안시스템 별 정책적용 현황을 관리하여야 한다.	조직에서 운영하고 있는 보안시스템 운영절차를 수립하고 있는가?	<ul style="list-style-type: none"> <li>보안시스템(정보보호시스템)은 정보통신망을 통하여 수집 • 저장 • 검색 및 송 • 수신되는 정보의 훼손 • 변조 • 유출 등을 방지하기 위한 장치로서 침입차단시스템(FW), 침입탐지시스템(IDS), 침입방지시스템(IPS), 웹방화벽, DB 접근통제시스템, 내부정보유출방지시스템(DLP), 가상사설망(VPN), 패치관리시스템(PMS) 등을 포함할 수 있다.</li> <li>외부침입 탐지 및 차단, 내외부자에 의한 정보유출 방지 등을 위하여 도입 • 운영하고 있는 보안시스템에 대한 운영절차를 수립하여야 한다.</li> <li>- 보안시스템 유형별 책임자 및 관리자 지정</li> <li>- 보안시스템 정책(룰셋 등) 적용(등록, 변경, 삭제 등) 절차</li> <li>- 최신 정책 업데이트: IDS, IPS 등의 보안시스템의 경우 새로운 공격기법을 탐지하기 위한 최신 패턴 및 엔진 지속적 업데이트</li> <li>- 보안시스템 이벤트 모니터링 절차: 정책에 위배되는 이상징후 탐지 및 확인 등</li> <li>- 보안시스템 접근통제 정책</li> <li>- 보안시스템 운영현황 주기적 점검 등</li> </ul>
		보안시스템 관리자 등 접근이 허용된 인원을 최소화하고 비인가자 접근을 엄격하게 통제하고 있는가?	<p>사용자 인증, 관리자 단말 IP 또는 MAC 접근 통제 등의 보호대책을 적용하여 보안시스템 관리자 등 접근이 허용된 인원 이외의 비인가자 접근을 엄격히 통제하여야 한다. 또 주기적인 보안시스템 접속로그 분석을 통해 비인가자에 의한 접근시도를 확인하고 적절한 조치를 하여야 한다.</p>
		보안시스템별 정책(룰셋 등) 신규 등록, 변경, 삭제 등 절차를 수립하고 정책의 타당성 검토를 주기적으로 수행하고 있는가?	<ul style="list-style-type: none"> <li>보안시스템별로 정책(룰셋 등) 신규 등록, 변경, 삭제 등을 위한 공식적인 절차(신청, 승인, 적용 등)를 수립 • 이행하여야 한다. 이는 정책(룰셋 등)의 생성 이력을 확인하기 위한 것이다.</li> <li>또한 정책의 타당성 및 적정성을 주기적으로 검토하여 다음 사항에 해당하는 경우 정책을 삭제 또는 변경하여야 한다.</li> <li>- 내부 보안정책 위배 (예: FW 룰셋 내부망 Inbound Any 정책 허용 등)</li> <li>- 미승인 정책</li> <li>- 장기간 미사용 정책</li> <li>- 중복 또는 사용 기간 만료 정책</li> <li>- 퇴직자 및 직무 변경자 관련 정책 등</li> </ul>

출처: ISMS 인증기준 세부 점검항목

<표 1-9> ISMS 인증기준 세부 점검 항목 중 11. 운영보안 - 보안시스템 운영

통제항목	목적	점검 항목	설명
원격 운영 관리	내부 네트워크를 통하여 정보시스템을 관리하는 경우 특정 단말에서만 접근을 할 수 있도록 제한하고, 원격지에서 인터넷 등 외부 네트워크를 통하여 정보시스템을 관리하는 것은 원칙적으로 금지하고 부득이한 사유로 인해 허용하는 경우에는 책임자 승인, 접속 단말 및 사용자 인증, 구간 암호화, 접속 단말 보안(백신, 패치 등) 등의 보호 대책을 수립하여야 한다.	내부 네트워크를 통해서 원격으로 시스템을 운영하는 경우 특정 단말에 한해서만 접근을 허용하고 있는가?	내부 네트워크를 통해 정보시스템(서버, 네트워크 장비, 정보보호시스템 등)을 운영하거나 웹관리자 페이지에 접속하는 경우 관리자는 지정된 단말을 통해서만 접근 할 수 있도록 통제(IP 또는 MAC 인증 등)하여야 한다. 특히 패드, 스마트폰 등 스마트기기를 통한 정보시스템 원격운영은 원칙적으로 금지하여야 한다. 다만 부득이한 경우 스마트기기에 대한 보안대책을 마련하고 책임자의 승인 후 사용하여야 한다.
		인터넷과 같은 외부 네트워크를 통한 정보시스템 원격운영은 원칙적으로 금지하고 있으며 부득이하게 허용하는 경우 다음과 같은 대책을 마련하고 있는가?  - 정보보호 최고책임자 승인 - 접속 단말 및 사용자 인증 - 한시적 접근권한 부여 - VPN 등의 전송구간 암호화 - 접속 단말 보안 - 원격운영 현황 지속적인 모니터링 등	<ul style="list-style-type: none"> <li>• 인터넷과 같은 외부 네트워크를 통한 정보시스템 원격운영은 원칙적으로 금지하여야 하며 긴급 장애 대응, 유지보수 등과 같이 부득이한 경우 다음과 같은 보안대책을 마련하여야 하여야 한다.</li> <li>- 원격운영에 대한 정보보호 최고책임자 승인 절차</li> <li>- 접속 단말 및 사용자 인증절차: ID/PW 이외의 강화된 인증방식(공인인증서, OTP 등) 적용 권고. 법적 요구사항 의무적 반영 필요.</li> <li>- 한시적 접근권한 부여: VPN 계정, 시스템 접근권한 등</li> <li>- VPN 등의 전송구간 암호화</li> <li>- 접속 단말 보안 (예: 백신 설치, 보안패치 적용 등)</li> <li>- 원격운영 현황(원격운영 인가자, VPN 계정 발급 현황 등) 지속적인 모니터링</li> <li>- 원격 접속 기록 로깅 및 주기적 분석</li> <li>- 원격운영 관련 보안인식교육 등</li> </ul> <p>※ 참고 ※</p> <ul style="list-style-type: none"> <li>- 정보통신망 이용촉진 및 정보보호 등에 관한 법률 '개인정보의 기술적 • 관리적 보호조치(고시)' 제4조(접근통제)</li> <li>- 개인정보 보호법 '개인정보의 안전성 확보기준(고시)' 제6조(접근통제 시스템 설치 및 운영)</li> </ul>

출처: ISMS 인증기준 세부 점검항목

<표 1-10> ISMS 인증기준 세부 점검 항목 중 11. 운영보안 - 무선 네트워크 보안

통제항목	목적	점검 항목	설명
무선네트워크 보안	무선랜 등을 통해 무선인터넷을 사용하는 경우 무선 네트워크 구간에 대한 보안을 강화하기 위해 사용자 인증, 송수신 데이터 암호화 등의 보호대책을 수립하여야 한다.	조직 내 무선네트워크 환경을 구축(AP 설치)할 경우 허가(승인), 보안성 검토 등 절차를 마련하고 구축에 따른 다음 (주요) 보호대책을 적용하고 있는가?	<ul style="list-style-type: none"> <li>• 조직 내부 네트워크에 연결이 가능한 무선네트워크 환경 구축 시에는 내부 승인 절차를 마련하여 비인가된 (사설)무선 네트워크 장비(Rogue AP: Access Point)를 운영하지 않도록 하여야 하며 사전 보안성 검토를 수행하여 다음과 같은 보호대책을 적용하여야 한다.</li> <li>- 무선네트워크 장비 접속 단말기 인증 및 보안</li> <li>- 무선네트워크 장비 (예: AP, Access Point) 보안 및 허용 장비 리스트</li> <li>- 무선 네트워크를 통하여 접근할 수 있는 정보시스템 범위 정의</li> <li>- 무선네트워크 사용권한 신청/변경/삭제 절차</li> <li>- 사용자 식별 및 인증</li> <li>- 무선네트워크 서비스 거리 제한 (주파수 세기 조정)</li> <li>- 정보송수신 시 무선망 암호화 기준 (예: WPA2)</li> <li>- 전산실 등 통제구역 내 무선네트워크 사용 제한</li> <li>- SSID(Service Set Identification) 브로드캐스팅 중지 및 추측 어려운 SSID 사용 등</li> </ul>
		- 무선네트워크 장비 (AP) 접속 단말 인증 (MAC 인증 등)	
		- 무선네트워크 장비 (AP) 정보 송수신 시 암호화 기능 설정 (WPA2 이상 권고)	
		- 무선네트워크 장비 (AP) SSID 숨김(브로드캐스팅 중지) 기능 설정	<ul style="list-style-type: none"> <li>• 내부 네트워크에 무선네트워크 환경을 구축하는 것은 업무의 편리성을 증대할 수는 있으나 충분한 보호 대책 마련 없이 적용할 경우 내부 정보유출, 해킹 등의 심각한 상황을 초래할 수 있으므로 업무상 반드시 필요한 경우를 제외하고는 매우 신중하게 접근하여야 한다.</li> </ul>
		정상적인 절차에 따라 무선네트워크 사용을 허가한 경우 인가된 임직원만 무선네트워크를 사용할 수 있도록 사용 신청 및 해지 절차를 수립하고 있는가?	<ul style="list-style-type: none"> <li>• 외부인이 무선네트워크 통해 내부 네트워크(업무망)에 접속할 수 없도록 인가받은 임직원만 무선네트워크를 사용할 수 있도록 필요한 절차를 마련하여야 한다.</li> </ul>
		외부인에게 제공하는 무선네트워크를 내부 네트워크(업무망)와 분리하고 있는가?	<ul style="list-style-type: none"> <li>• 회의실, 교육장, 기자실, 민원실 등 외부인의 접근이 빈번한 장소인 경우 외부인에게 무선네트워크 사용을 허용할 수 있으나 내부 네트워크(업무망)와 분리하여 무선네트워크를 통한 내부 네트워크 침투 및 내부 정보유출을 방지하여야 한다.</li> </ul>

출처: ISMS 인증기준 세부 점검항목

4. PIMS 인증기준 상의 네트워크 보안 관련 기준을 확인한다.

개인정보 보호법 제32조2항에 따른 PIMS 인증과 관련하여 인증기준 상의 네트워크 보안과 관련된 기준을 확인한다.

(1) 한국인터넷진흥원 웹사이트를 통해 PIMS 인증기준의 네트워크 보안 관련 기준을 확인한다.

한국인터넷진흥원의 PIMS 지원 웹사이트를 통해 PIMS 인증기준을 검색하고 네트워크 보안 관련 기준을 확인한다.

(가) PIMS 지원 웹사이트에 접속한다.

한국인터넷진흥원에서 운영하는 PIMS지원 웹사이트(<http://pims.kisa.or.kr>)에 접속한다.



출처: 인터넷진흥원(<http://pims.kisa.or.kr>) 2018.5.31. 스크린샷  
[그림 1-9] PIMS지원 웹사이트 접속화면

(나) PIMS 인증기준을 검색한다.

PIMS 자료실 검색창에 ‘인증기준’을 입력하고 검색을 클릭하여 PIMS 인증기준을 다운로드한다.



https://isms.kisa.or.kr/main/pims/notice/?mode=list&boardId=1 KISA 정보보호 및 개인정보...

심사원로그인 금자크기 사이트맵 KISA운영 홈페이지 보기

KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY

ISMS PIMS 정보보호등급제 클라우드 보안인증제 온라인학습 알림마당

Home > PIMS > 자료실

### 자료실

안전한 개인정보보호 관리체계를 만들어갑니다.

#### PIMS 자료실

전체 인증기준 전체 검색

총 3 (1/1)

번호	구분	제목	등록일	조회	첨부
3	자료	PIMS 인증기준 세부점검항목(2016.11.09)	2016-11-09	13029	
2	자료	PIMS(PIMS-PPL) 제도 통합예(다른 인증신청서 및 2016...	2016-01-18	8688	
1	가이드	15.03.05 개인정보보호관리체계(PIMS) 인증신청가이드...	2015-03-05	2998	

출처: 인터넷진흥원(<http://pims.kisa.or.kr/>) 2018.5.31. 스크린샷  
[그림 1-10] PIMS 인증기준 세부 점검항목

(다) PIMS 인증기준 세부 점검항목 중 네트워크 보안 관련 기준을 확인한다.

ISMS 인증기준 세부 점검항목 중 개인정보 보호대책 분야에서 네트워크 보안 관련 내용을 확인한다.

1) PIMS 인증 기 세부 점검항목 중 10. 접근통제 분야에서 네트워크 보안 관련 내용을 확인한다.

네트워크에 대한 비인가 접근을 통제하기 위한 접근통제 리스트, IP 등 식별자에 대한 관리체계를 수립하고, 내/외부 네트워크를 분리해야 함을 확인한다.

<표 1-11> PIMS 인증기준 세부 점검 항목 중 개인정보 보호대책 - 접근통제영역관리 - 네트워크 접근

인증기준	상세 내용	세부 점검 항목
8.3 접근통제 영역관리	8.3.1 네트워크 접근	접근통제 정책에 따라 인가된 사용자만이 네트워크에 접근할 수 있도록 네트워크 식별자(IP) 할당 등을 통제하고 있는가?
		네트워크 구성 변경 시에는 공식적인 변경 관리 절차를 준수하고 자체적인 보안성 검토를 수행하고 있는가?
		네트워크 대역별 IP 주소 부여 기준을 마련하여 DB서버 등 외부 연결이 필요하지 않은 경우 사설 IP로 할당하는 등의 대책을 적용하고 있는가?
		서비스, 사용자 그룹, 정보자산의 중요도, 법적 요구사항에 따라 네트워크 영역을 물리적 또는 논리적으로 망을 분리하고 있는가?
		물리적으로 떨어진 IDC 센터, 지사, 대리점, 협력업체, 고객센터 등과의 네트워크 연결 시 전용회선을 구축 또는 VPN(가상사설망) 등을 활용하고 있는가?
		네트워크 장비(라우터, 스위치 등)별로 접근이 허용된 사용자를 명확하게 식별·인증하고 안전한 접근수단을 적용하고 있는가?
		조직 내 무선네트워크 환경을 구축(AP 설치)할 경우 내부 승인, 보안성 검토 등 절차를 마련하고 구축에 따른 다음 사항을 보호대책에 적용하고 있는가?
		<ul style="list-style-type: none"> <li>- 접속 단말 인증 방안(MAC 인증 등)</li> <li>- 정보 송수신 시 암호화 기능 설정(WPA2 이상 권고)</li> <li>- SSID 숨김(브로드캐스팅 중지) 기능 설정</li> <li>- 무선 AP의 관리자 접근 통제 (IP 등)</li> <li>- 무선 AP의 관리자 패스워드 주기적 변경 등</li> </ul>
		정상적인 절차에 따라 무선네트워크 사용을 허가한 경우 인가된 임직원만 무선네트워크를 사용할 수 있도록 사용 신청 및 해지 절차를 수립하여 운영하고 있는가?

출처: PIMS 인증기준 세부 점검항목

<표 1-12> PIMS 인증기준 세부 점검 항목 중 개인정보 보호대책 - 접근통제영역관리 - 원격운영 접근

인증기준	상세 내용	세부 점검 항목
8.3 접근 통제영역 관리	8.3.5 원격 운영 접근	<p>내부 네트워크를 통해서 원격으로 개인정보처리시스템 및 개인정보 처리와 연관된 주요 자산(서버, 네트워크 장비, 보안장비 등)을 운영하는 경우 특정 단말에 한해서만 접근을 허용하고 있는가?</p> <p>인터넷과 같은 외부 네트워크를 통한 개인정보처리시스템 및 개인정보 처리와 연관된 주요 자산(서버, 네트워크 장비, 보안장비 등)의 원격운영은 원칙적으로 금지하고 있으며 부득이하게 허용하는 경우 다음과 같은 대책을 마련하고 있는가?</p> <ul style="list-style-type: none"> <li>- 책임자 승인</li> <li>- 접속 단말 및 사용자 인증</li> <li>- 한시적 접근권한 부여</li> <li>- VPN 등의 전송구간 암호화</li> <li>- 접속 단말 보안</li> <li>- 원격운영 현황 지속적인 모니터링 등</li> </ul> <p>정보통신망을 통해 외부에서 개인정보처리시스템에 접속하여 개인정보 파일을 다운로드하거나 출력 시 통제 기준을 수립하여 이행하고 있는가?</p>

출처: PIMS 인증기준 세부 점검항목

<표 1-13> PIMS 인증기준 세부 점검 항목 중 개인정보 보호대책 - 접근통제영역관리 - 인터넷 접속통제

인증기준	상세 내용	세부 점검 항목
8.3 접근 통제영역 관리	8.3.6 인터넷 접속통제	<p>개인정보처리시스템에 접근 가능한 개인정보취급자의 PC 등 인터넷 접속에 대한 정책을 수립 및 이행하고 있는가?</p> <ul style="list-style-type: none"> <li>- 인터넷 연결 시 네트워크 구성 정책</li> <li>- 이메일, 인터넷 사이트의 접속, 소프트웨어 다운로드 및 전송 등의 사용자 접속정책</li> <li>- 유해사이트(성인, 오락 등) 접속 차단 정책</li> <li>- 정보 유출 가능 사이트(웹하드, P2P 등) 접속 차단 정책</li> <li>- 인터넷 접속내역 검토(모니터링) 정책 등</li> </ul> <p>주요 개인정보취급자(권한부여자, 개인정보 삭제 및 다운로드 가능자)를 식별하여 인터넷 접속을 제한하고 있는가?</p> <p>아래의 내용을 포함하는 개인정보처리시스템 운영 절차를 마련하였는가?</p> <ul style="list-style-type: none"> <li>- 문제 발생 시 재동작, 복구 절차</li> <li>- 오류 및 예외사항 처리 방안</li> <li>- 악성코드 통제</li> <li>- 보안시스템 운용</li> <li>- 모바일 기기 관리</li> <li>- 패치관리 등</li> </ul>

출처: PIMS 인증기준 세부 점검항목

<표 1-14> PIMS 인증기준 세부 점검 항목 중 개인정보 보호대책 - 운영보안 - 보안시스템 설치운영

인증기준	상세 내용	세부 점검 항목
8.4 운영보안	8.4.6 불법적인 접근 및 침해 사고 방지를 위해 침입 차단 및 탐지 기능을 포함한 시스템을 설치·운영하여야 한다. 또 보안 시스템 운영절차를 수립하고 보안시스템별 정책 적용 현황을 관리하여야 한다.	불법적인 접근 및 침해사고 방지를 위하여 보안 시스템을 설치·운영하고 있는가?
		외부침입 탐지 및 차단, 내외부자에 의한 정보유출 방지 등을 위하여 도입·운영하고 있는 보안시스템에 대한 운영절차를 수립하여 운영하고 있는가?
		- 보안시스템 유형별 책임자 및 관리자 지정 - 보안시스템 정책(룰셋 등) 적용(등록, 변경, 삭제 등) 절차 - 보안시스템 이벤트 모니터링 절차 - 보안시스템 접근통제 정책 - 보안시스템 운영현황 주기적 점검 등
		사용자 인증, 관리자 단말 IP 또는 MAC 접근통제 등의 보호대책을 적용하여 보안시스템 관리자 등 접근이 허용된 인원 이외의 비인가자 접근을 엄격히 통제하고, 주기적인 보안시스템 접속로그 분석을 통해 비인가자에 의한 접근시도를 확인하고 적절한 조치를 취하고 있는가?
		보안시스템 특성에 따른 정책(룰셋 등)의 신규 등록, 변경, 삭제, 백업 등 절차를 수립하고 정책의 타당성 검토를 주기적으로 수행하고 있는가?
		보안시스템의 예외 정책 등록에 대하여 절차에 따라 관리하고 있으며, 예외 정책 사용자에 대하여 최소한의 권한으로 관리하고 있는가?

출처: PIMS 인증기준 세부 점검항목

② 국내 규제 및 가이드 기준을 기반으로 하여 네트워크 보안 요구사항을 정의한다.

각종 법률 및 시행령과 ISMS/PIMS 인증기준에서 요구하고 있는 네트워크 보안 설계 요구사항을 통합하여 명세한다.

1. 네트워크 보안 설계와 관련된 요구사항을 도출하고 검토한다.

정보통신망법, 개인정보 보호법 및 ISMS/PIMS등 각종 기준에서 가이드하고 있는 네트워크 설계에 대한 요구사항을 도출하고 검토한다.

(1) 서버 네트워크 설계 요구사항을 도출하고 검토한다.

각종 기준에서 가이드하고 있는 네트워크 설계에 대한 요구사항과 사이버 침해공격 대응을 위한 요구사항을 포함하여 서버 네트워크 분야의 보안 설계 요구사항을 정의한다.

(2) 클라이언트 네트워크 설계 요구사항을 도출하고 검토한다.

각종 기준에서 가이드하고 있는 네트워크 설계에 대한 요구사항 중 PC 혹은 무선 네트워크와 같은 클라이언트 네트워크 설계 요구사항을 정의한다.

(3) 네트워크 보안의 운영관리 체계와 관련된 요구사항을 도출하고 검토한다.

각종 기준에서 가이드하고 있는 네트워크 설계에 대한 요구사항 중 운영 보안 체계 관련 요구사항을 정의한다.

<표 1-15> 네트워크 보안 요구사항 도출 및 검토

구분	도출 항목
서버 네트워크 보안 요구사항	(가) 시스템에 대한 접속권한을 IP 주소 등으로 제한하여 허가받지 않은 접근을 제한할 수 있어야 한다.
	(나) 시스템에 접속한 IP 주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지할 수 있어야 한다.
	(다) 특정 컴퓨터를 물리적 또는 논리적으로 인터넷과 차단(망분리)할 수 있어야 한다.
	(라) 외부망에서 시스템에 접속하려는 경우를 위해 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용할 수 있어야 한다.
	(마) 원격지에서 인터넷 등 외부 네트워크를 통하여 정보시스템을 관리하는 것은 원칙적으로 금지하고 부득이한 사유로 인해 허용하는 경우에는 책임자 승인, 접속 단말 및 사용자 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등의 보호대책을 수립해야 한다.
	(바) 서비스, 사용자 그룹, 정보자산의 중요도에 따라 내·외부 네트워크를 분리하여야 한다.
	(사) DDoS 공격 등에 대해 방어할 수 있어야 한다.
	(아) 인터넷 및 이메일 서버 구간에 대해 악성코드의 유입을 차단할 수 있어야 한다.
	(자) 서버 네트워크를 통한 개인정보의 유출을 탐지 및 차단할 수 있어야 한다.
	(가) 허가받지 않은 단말의 네트워크 접속을 차단할 수 있어야 한다.
클라이언트 네트워크 보안 요구사항	(나) 내부 네트워크를 통하여 정보시스템을 관리하는 경우 특정 단말에서만 접근을 할 수 있도록 제한해야 한다.
	(다) 무선랜 등을 통해 무선인터넷을 사용하는 경우 무선 네트워크 구간에 대한 보안을 강화하기 위해 사용자 인증, 송수신 데이터 암호화 등의 보호대책을 수립해야 한다.
	(라) 중요 시스템에 접근 가능한 PC는 인터넷 접속 또는 서비스를 제한 및 통제하고, 필요 시 인터넷 접속내역을 모니터링할 수 있어야 한다.
네트워크 운영 보안 요구사항	(가) 보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립하고 보안시스템별 정책적용 현황을 관리할 수 있어야 한다.
	(나) 네트워크에 대한 비인가 접근을 통제하기 위해 필요한 네트워크 접근 통제리스트, 네트워크 식별자 등에 대한 관리절차를 수립해야 한다.

2. 검토가 완료된 네트워크 보안 요구사항을 명세하여 작성한다.

네트워크 보안 관련 이해관계자의 검토가 완료된 네트워크 설계에 대한 보안 요구사항을 명세하여 작성한다.

<표 1-16> 네트워크 보안 요구사항명세서

구분	보안 요구사항	ID	비고
서버 네트워크	시스템에 대한 접속권한을 IP 주소 등으로 제한하여 허가받지 않은 접근을 제한할 수 있어야 한다.	S-0001	
	시스템에 접속한 IP 주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지할 수 있어야 한다.	S-0002	
	특정 컴퓨터를 물리적 또는 논리적으로 인터넷과 차단(망분리)할 수 있어야 한다.	S-0003	
	외부망에서 시스템에 접속하려는 경우를 위해 가상사설망(VPN: Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용할 수 있어야 한다.	S-0004	
	원격지에서 인터넷 등 외부 네트워크를 통하여 정보시스템을 관리하는 것은 원칙적으로 금지하고 부득이한 사유로 인해 허용하는 경우에는 책임자 승인, 접속 단말 및 사용자 인증, 구간 암호화, 접속단말 보안(백신, 패치 등) 등의 보호대책을 수립해야 한다.	S-0005	
	서비스, 사용자 그룹, 정보자산의 중요도에 따라 내·외부 네트워크를 분리하여야 한다.	S-0006	
	DDoS 공격 등에 대해 방어할 수 있어야 한다.	S-0007	
	인터넷 구간 및 이메일 서버 구간에 대해 악성코드의 유입을 차단할 수 있어야 한다.	S-0008	
	서버 네트워크를 통한 개인정보의 유출을 탐지 및 차단할 수 있어야 한다.	S-0009	
클라이언트 네트워크	허가받지 않은 단말의 네트워크 접속을 차단할 수 있어야 한다.	C-0001	
	내부 네트워크를 통하여 정보시스템을 관리하는 경우 특정 단말에서만 접근을 할 수 있도록 제한해야 한다.	C-0002	
	무선랜 등을 통해 무선인터넷을 사용하는 경우 무선 네트워크 구간에 대한 보안을 강화하기 위해 사용자 인증, 송수신 데이터 암호화 등의 보호대책을 수립해야 한다.	C-0003	
	중요 시스템에 접근 가능한 PC는 인터넷 접속 또는 서비스를 제한 및 통제하고, 필요 시 인터넷 접속내역을 모니터링할 수 있어야 한다.	C-0004	
운영 보안	보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립하고 보안시스템별 정책적용 현황을 관리할 수 있어야 한다.	O-0001	
	네트워크에 대한 비인가 접근을 통제하기 위해 필요한 네트워크 접근통제리스트, 네트워크 식별자 등에 대한 관리절차를 수립해야 한다.	O-0002	

3. 작성 완료된 네트워크 보안 요구사항명세서를 승인하여 확정한다.

보안 요구사항명세서를 최종 승인하고 확정하여 필요 시 관련 부서에 배포한다.

**수행 tip**

- 요구사항명세서는 추후 구현 및 테스트과정에서 활용할 수 있도록 요구사항추적표를 후속작성하여 관리하는 것이 바람직하다.

## 1-2. NW보안 설계

### 학습 목표

- 명세된 보안 요구사항을 만족하는 네트워크를 설계할 수 있다.

### 필요 지식 /

#### ① 네트워크 보안 설계 원칙 및 보안 장비 유형

##### 1. 네트워크 보안 설계 원칙

###### (1) 최소화의 원칙(Minimalization)

보안의 핵심 원칙은 최소화라고 할 수 있다. 반드시 필요한 항목을 필요로 하는 사람에게 최소한의 기간 동안만 접근을 허용하는 것으로써, 이는 네트워크 접근통제와 관련된 기본적 원칙이라고 할 수 있다.

###### (2) 분리의 원칙(Isolation)

분리는 리스크를 격리시키기 위해 필요하다. 네트워크 설계 시 외부에서 접근하는 DMZ와 외부에서 접근 불가능한 사설 IP 기반의 내부망의 분리 혹은 개발 서버 영역과 운영 서버 영역의 분리가 그 예이다. 또 권한을 가진 업무처리자와 권한을 부여하는 관리자의 권한 분리도 분리의 예라고 할 수 있다.

###### (3) 다중 보안의 원칙(Defence in Depth)

보안 위협의 대응차원에서 보안 대책을 정의하고 구현하게 되는데, 하나의 보안 대책이 무력화되더라도 다른 보안 대책을 통해 전체적인 보안성이 확보되도록 하는 개념이다. 외부로부터 공격자가 내부로 침입하여 중요 개인정보를 유출하는 위협 시나리오에 대해서 보안 시스템을 통해 침입을 방지하는 체계(1차)와 내부 서버 사이에 확산 침투를 방지하는 체계(2차), 그리고 정제된 개인정보를 외부로 유출하는 것을 방지하는 체계(3차) 등 총 3중 보안대책이 적용된다면 그중 하나의 보안대책이 무력화되더라도 나머지 유효한 보안대책을 통해 개인정보 유출을 방지할 수 있다.

###### (4) 법규 준수의 원칙(Compliance)

보안 리스크를 줄이기 위함과 동시에 법률 위반을 방지하기 위해 법규에서 가이드하는 보안대책은 반드시 적용이 필요하다.



## 2. 네트워크 보안 장비 유형

네트워크 보안장비는 접근통제, 침입차단 및 탐지, DDoS 탐지 등을 수행하는 일체형 장비들이 포함된다.

<표 1-17> 주요 보안장비

용어	의미
방화벽(Fire Wall)	외부에서 내부, 내부에서 외부의 정보통신망에 불법으로 접근하는 것을 차단하는 시스템으로써 전송 정보의 발신지와 수신지에 대한 IP 주소와 포트 번호에 대한 접근통제를 수행한다.
침입탐지시스템(IDS)	침입탐지시스템(IDS, Intrusion Detection System)은 네트워크를 통한 사이버 공격을 실시간으로 탐지한다.
침입예방시스템(IPS)	침입예방시스템(IPS, Intrusion Prevention System)은 네트워크를 통한 사이버 공격을 실시간으로 탐지하고 차단한다.
DDoS방지시스템	목적지를 기반으로 트래픽이 임계치를 초과할 경우 기존의 세션을 제외한 패킷을 Null Routing처리하여 DDoS를 통한 공격에 대응한다.
웹방화벽	알려진 유형의 웹 해킹 공격을 탐지하고 방어한다.

<표 1-18> 방화벽 주요 기능

기능	설명	OSI 계층
패킷 필터	비인가 Packet 차단	L3, L4
상태 확인	세션 정보 연계(FTP, TFTP, H.323, SIP ...)	L4
주소 변환	IP Header 변경(NAT, DHCP)	L4
트래픽 관리	트래픽 용량 관리(bps, sps, cps)	L4
프록시	HTTP, SMTP, POP3, SQL, etc	L3, L4
콘텐츠 필터	HTTP, SMTP, POP3	L7
URL 필터	Web Paging Redirect	L7
바이러스 필터	Mail, Web File Download Check	L7
MAC 바인딩	IP/MAC Address Mapping	L2, L3
영역 분리	Network Address 구간(Subnet/Group) 관리	L3
운영 모드	Router/Bridge Mode	L2, L3

<표 1-19> IDS와 IPS의 차이

항목	IDS	IPS
Layer	애플리케이션	커널
탐지 기준	Signature	
차단 방식	제한적 TCP 리셋 간접차단 - 방화벽 연동	패킷 드랍
제공 기능	탐지/로그 기록	탐지/로그 기록, 임계치 설정
탐지 범위	넓음(Application Memory)	상대적으로 적음(Kernel Memory)
탐지 성능	늦음(I/O Processing 지연 발생)	빠름
안정성	네트워크 장애 발생 무관	장애 시 로컬 네트워크 장애 발생
지원 기술	미러링	후킹
동작 방식	탭 모드	인라인 모드
탐지 위치	라우터 트래픽	로컬 트래픽

## ② 망분리의 개념 및 유형

### 1. 망분리의 개념 및 근거

#### (1) 망분리의 개념

시스템의 오용/악용으로부터 정보 시스템을 보호하기 위한 것으로써, 중요 내부 업무 처리를 수행하는 자의 PC나 노트북을 인터넷 접속이 되지 않도록 차단하는 기술이다.

#### (2) 망분리의 근거

개인정보의 기술적 관리적 보호조치 기준 제4조(접근통제) 6항에 따르면 ‘전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만 명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자 등은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근 권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하여야 한다.’ 라고 되어있는 부분을 그 근거로 하고 있다.

## 2. 망분리의 유형 및 구현 방식

### (1) 망분리의 유형

망분리의 유형은 크게 물리적 혹은 논리적 망분리로 구현가능하다.

#### (가) 물리적 망분리

물리적으로 2대 이상의 PC와 별도 회선으로 내부망과 외부망을 분리하는 방식이다.

#### (나) 논리적 망분리

한 대의 PC에서 가상화 기술을 이용하여 내부망과 외부망을 분리하는 방식이다.

### (2) 망분리의 세부 구현 방식

<표 1-20> 망분리의 구현 유형

분류		개념
물리적 망분리	2PC	개인이 업무용, 인터넷용 PC 별도로 나누어 사용하는 방식
	공용PC	2PC 방식과 동일하나 인터넷용 PC는 공유
논리적 망분리	서버 기반	업무 기본형 로컬 PC는 업무망 전용으로 동작
		인터넷 접속 시 별도 서버에서 인터넷용 가상 머신이 동작
	가상화 기반	인터넷 기본형 로컬 PC는 인터넷 전용으로 동작
		업무망 접속 시 별도 서버에서 업무망 접속용 가상 머신 동작
	Host 기반	로컬 PC는 업무망용 랜카드와 인터넷용 랜카드 별도 존재
		업무 기본형 로컬 PC는 업무용 PC로 동작하고 업무망용 랜카드로 통신
	가상화 기반	인터넷 기본형 로컬 PC는 인터넷용 PC로 동작하고 인터넷용 랜카드로 통신
		업무망 접속 시 로컬 PC에서 업무망용 가상 머신을 실행, 업무망용 가상머신은 업무망용 랜카드로 통신

## 수행 내용 / NW보안 설계하기

---

### 재료 · 자료

- 정보통신망 이용촉진 및 정보보호 등에 관한 법률
- 개인정보 보호법
- 정보보호관리체계에 관한 국제 표준 규격(ISO27001)
- 정보보호관리체계(ISMS) 인증기준 세부 점검항목
- 개인정보보호관리체계(PIMS) 인증기준 세부 점검항목

### 기기(장비 · 공구)

- 인터넷
- 컴퓨터
- 프린터
- 문서 작성 도구

### 안전 · 유의 사항

- 각종 규제 기준과 가이드를 통해 도출된 보안 요구사항을 준수할 수 있도록 네트워크 보안 설계를 순차적으로 진행한다.
- 방화벽, IPS 등 관문 네트워크 보안 체계와, 클라이언트 네트워크 보안 체계 및 운영 보안 체계가 설계에 반영되어야 한다.

### 수행 순서

① 명세된 보안 요구사항을 만족하는 네트워크를 설계한다.

서버 네트워크 분야와 사용자 단말기 네트워크 분야에 대해 네트워크 보안 설계를 수행한다.

1. 서버 네트워크 분야에 대한 네트워크 보안 설계를 수행한다.

서비스 제공을 위한 서버가 배치되는 서버 네트워크에 대한 보안설계를 수행한다.

(1) 네트워크 관문 영역에 대한 보안 설계를 수행한다.

서버팜이 인터넷과 연결되는 관문에 대한 보안 설계를 수행한다.

(가) 인가되지 않은 접근을 제한할 수 있는 방화벽을 구성한다.

방화벽을 네트워크의 내외부 경계에 구축하여 기본적인 접근통제를 구현한다.

(나) 접속 내역을 분석하여 불법적인 접근 시도를 탐지/차단할 수 있는 IPS를 구성한다.

불법 접속을 탐지하고 자동으로 차단할 수 있는 IPS를 구성한다.

(다) 대용량 DDoS 공격을 방어할 수 있는 Anti DDoS 솔루션을 구성한다.

방화벽의 앞 단에서 DDoS 공격에 대응하여 과다 세션을 처리할 수 있는 Anti DDoS 시스템을 구성한다.

(라) 웹 공격을 방어할 수 있는 웹방화벽을 구성한다.

웹 해킹공격을 탐지하고 방어할 수 있는 웹방화벽을 구성한다.

(마) 외부망으로부터의 악성코드 유입 방지 솔루션을 구성한다.

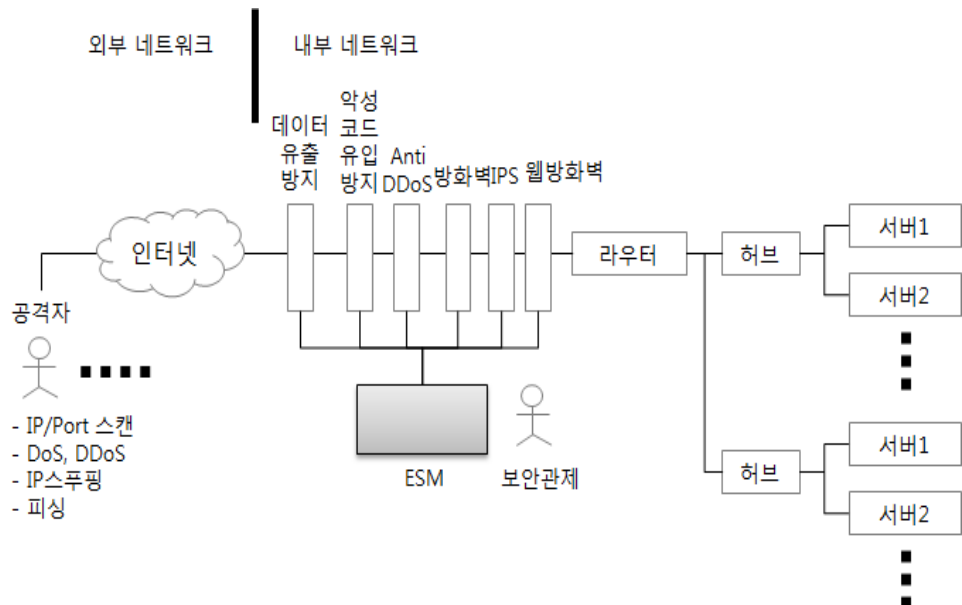
인터넷 혹은 이메일 수신 등을 통해 유입되는 악성 코드를 탐지하고 차단할 수 있는 솔루션을 구성한다.

(바) 외부망으로의 개인정보 유출 방지 솔루션을 구성한다.

내부망의 개인정보가 인터넷으로 유출되는 것을 탐지하고 차단할 수 있는 데이터 유출방지 솔루션을 구성한다.

(사) 보안 관제를 수행할 수 있는 ESM 솔루션을 구성한다.

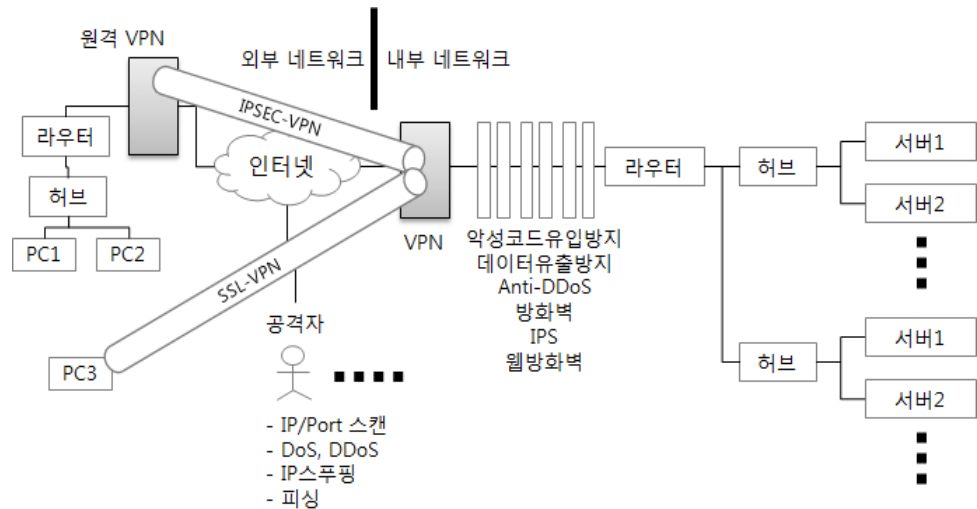
각종 보안 시스템으로부터 로그를 전송받아 IDS를 통해 불법 접속을 탐지하거나 IPS를 적용하여 자동 차단되도록 선택적으로 설계할 수 있다.



[그림 1-11] 관문 보안 솔루션 및 통합 보안 관제 체계 구성

(아) 외부망으로부터의 안전한 원격 접속을 제공하는 VPN 솔루션을 용도에 맞게 구성한다.

인터넷을 통해 외부 네트워크와 내부 네트워크를 연계하는 IPsec-VPN을 구성하거나, 외부망에 존재하는 PC와 내부망을 인터넷을 통해 연계하는 SSL-VPN을 구성한다.



[그림 1-12] VPN을 통한 외부망으로부터의 원격 접속 체계 구현

<표 1-21> IPsec VPN과 SSL-VPN의 비교

항목	IPsec	SSL
암호 위치	커널 - 3 계층	애플리케이션 - 5 계층
성능	상대적 빠름	IPSec-VPN의 1/4정도
IP Address	고정형	가변형
대상	지정된 서버-클라이언트	지정된 서버와 불특정 다수 사용자
배포 방식	사용자 PC 설치 없음	사용자 PC 설치(Active-X)
인증 방식	IKE기반 -X.509인증서, Pre-Shared Key	ID/Password
Routing변경	없음	정적 라우팅 경로 추가

(2) 서버 네트워크의 영역을 구분하는 보안 설계를 수행한다.

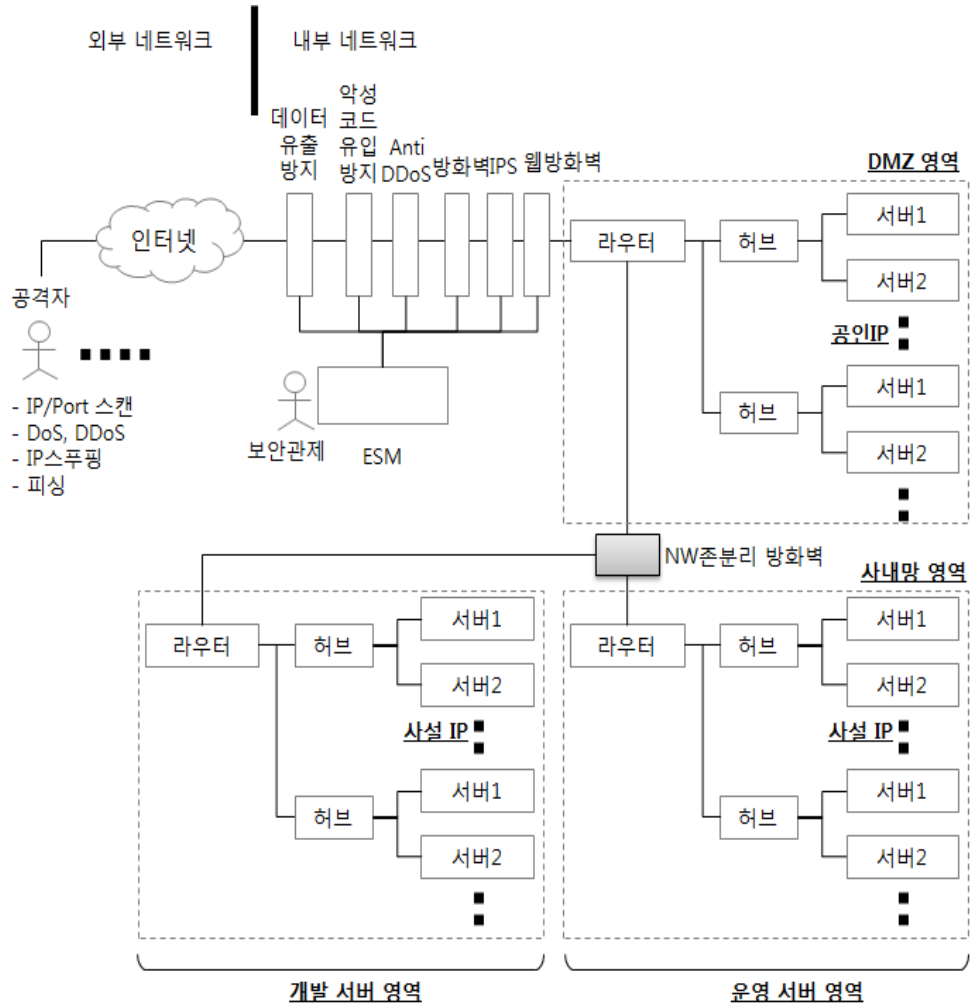
서버 네트워크 영역 별 상호 접근통제를 위한 보안 설계를 수행한다.

(가) DMZ영역과 내부망을 구분한다.

외부로부터의 접근이 불가피한 웹서버, 메일서버 등의 공개용 서버가 배치되는 DMZ 영역과 외부로부터의 직접 접근이 차단되는 내부망을 구분하여 설계한다. DMZ영역과 내부망 영역은 존 분리 방화벽으로 접근통제를 적용한다.

(나) 운영 서버 영역과 개발 서버 영역을 구분한다.

운영서버 영역과 개발서버 영역 또한 분리하여 설계해야 한다. 운영서버 영역과 개발서버 영역 간에 방화벽으로 접근통제를 적용한다.



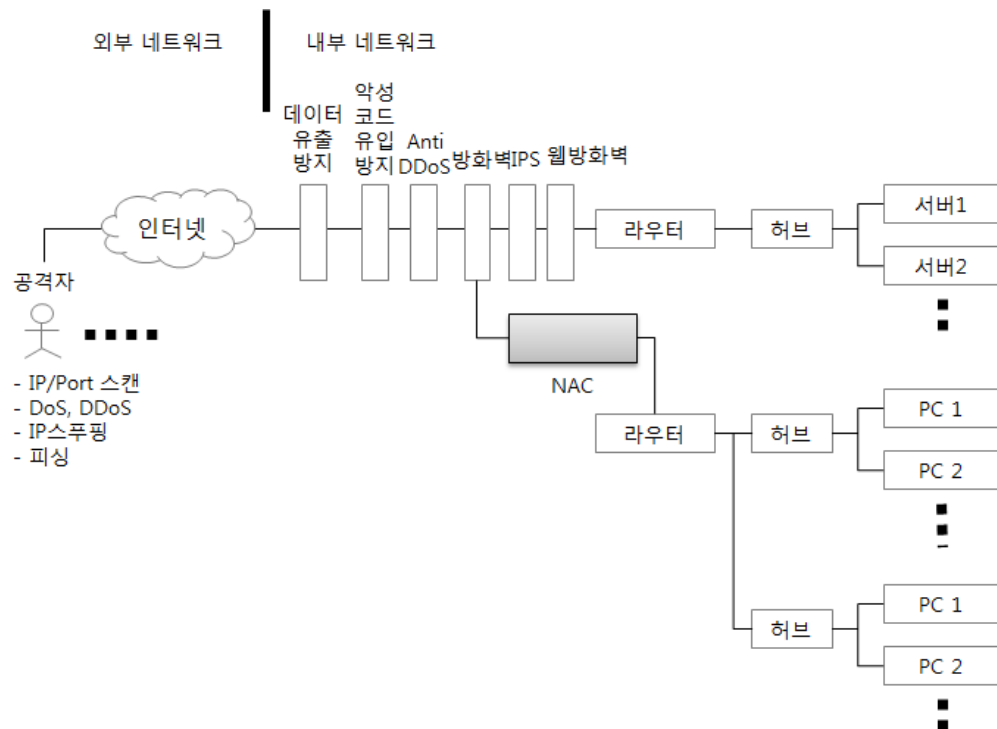
[그림 1-13] 존 분리 방화벽을 통한 개발 운영 네트워크 분리 구현

## 2. 사용자 단말기 네트워크 분야에 대한 네트워크 보안 설계를 수행한다.

사용자 단말기(PC/노트북)의 네트워크 접근 통제 및 망분리 요건을 준수하기 위한 보안설계를 수행한다.

### (1) 사용자 단말기(PC/노트북)의 접근통제를 위한 솔루션을 구성한다.

사전에 네트워크 접속이 승인된 단말기만의 접근을 허용하고 그 외의 단말기에 대한 네트워크 접속을 차단할 수 있는 네트워크 접근 통제(NAC, Network Access Control) 솔루션을 구성한다.



[그림 1-14] NAC을 통한 사용자 단말기의 네트워크 접근 통제 체계 구현

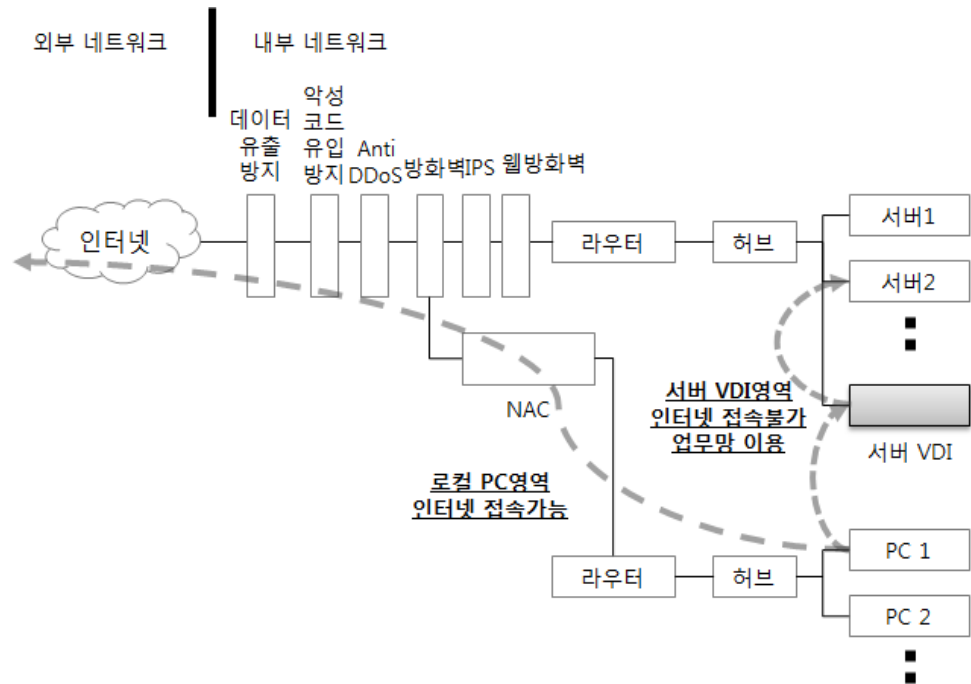
<표 1-22> NAC 제공 기능

기능 항목	주요 내용	비고
패치	OS 보안 업데이트	패치관리 시스템 연동
백신	악성 코드 감염 탐지/치료	
격리	Host 격리 (네트워크 인터페이스 차단)	일정 주기별 체크
패턴 업데이트	악성 코드 시그니처 업데이트	제로 데이 공격 대응
패턴 분석	악성 코드 전송 및 분석	
애플리케이션 통제	비인가 SW 설치 방지	라이선스 통제 병행
자원 관리	네트워크, CPU, 메모리 사용률 등 자원 관리	
호스트 인증	사용자 시스템 인증	비인가 시스템 네트워크 접속 불가

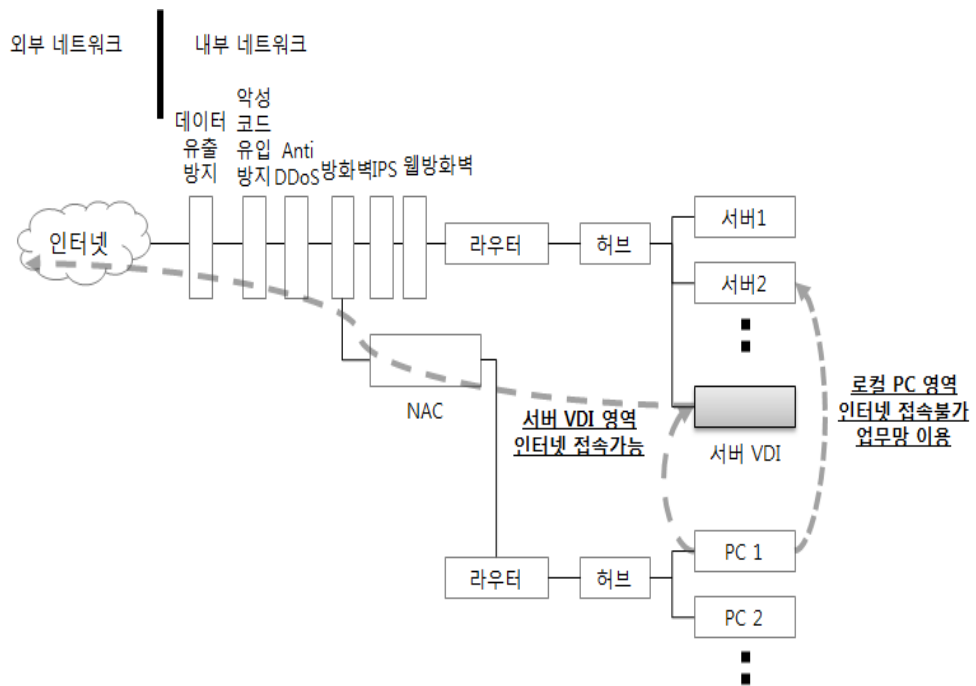
(2) 사용자 단말기에 대한 망분리 솔루션을 구성한다.

보안 관점에서 호스트 기반의 망분리보다 서버 기반의 논리적 망분리가 통제 무력화 방지 관점에서 더 적절하며, 서버에 VDI를 구성하도록 설계한다. 로컬 PC영역과 서버 내 VDI로 구성된 영역이 논리적으로 분리되고 관리자의 승인이 없을 경우에는 영역 간 파일의 전달을 차단한다. 문서 중앙화 관점에서 로컬 PC가 인터넷 접속이 되고 VDI환경을 업무환경으로 활용하는 경우가 일반적이다(서버기반 논리적 망분리 - 인터넷 기본형). 비용절감 관점에서 호스트 기반 가상화로 망분리를 구성하는 것도 가능하나 매체제어 솔루션 및 NAC 솔루션을 연계하여 망분리 무력화를 방지한다.

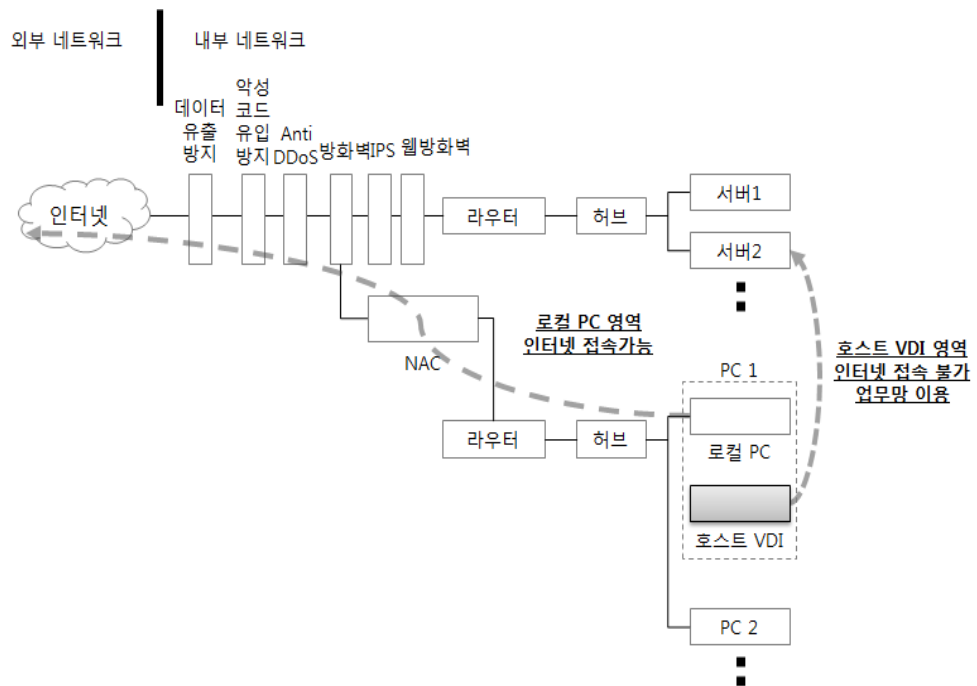




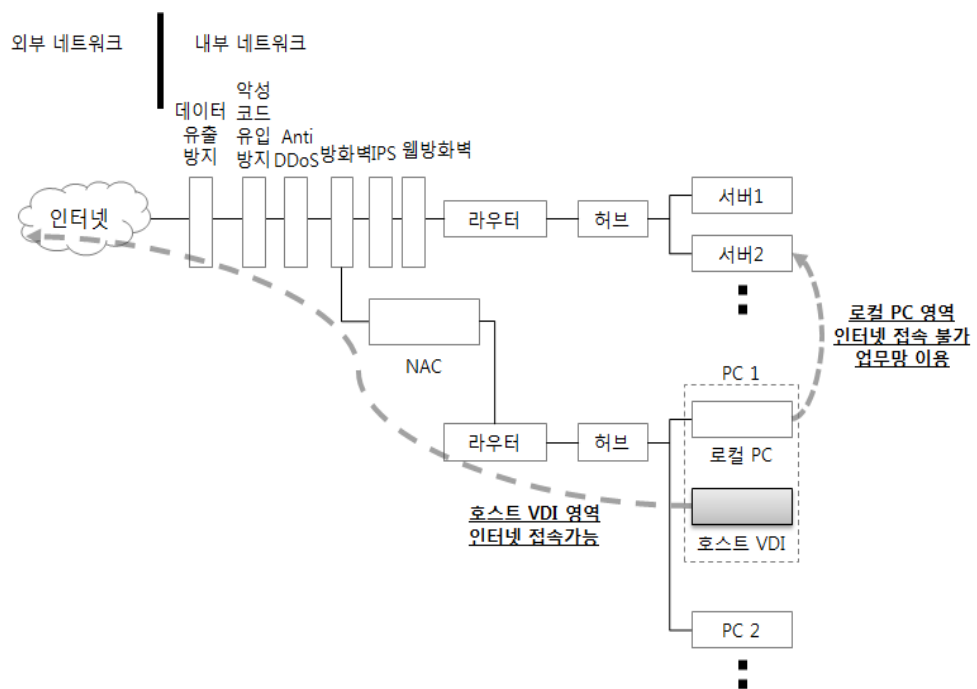
[그림 1-15] 서버기반 논리적 망분리 - Internet 기본형(일반적 구성)



[그림 1-16] 서버기반 논리적 망분리 - 업무망 기본형



[그림 1-17] 호스트 기반 논리적 망분리 - Internet 기본형



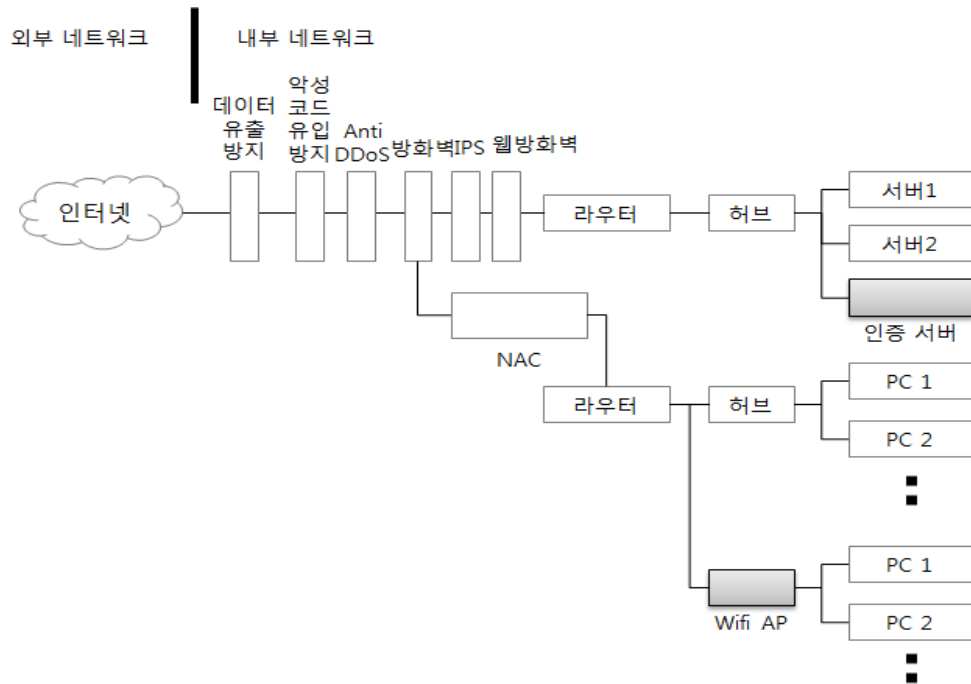
[그림 1-18] 호스트 기반 논리적 망분리 - 업무망 기본형

(3) 클라이언트 무선 네트워크에 대한 설계를 수행한다.

무선랜 등을 통해 무선인터넷을 사용하는 경우 무선 네트워크 구간에 대한 보안 적용을 위해 사용자 인증, 송수신 데이터 암호화 등의 보호 대책을 수립한다.

(가) 와이파이 접속점(Wifi AP, Wifi Access Point)을 구성하고 인증 시스템을 구성한다.

와이파이 연결이 더 효율적인 경우 제한적으로 와이파이 AP를 통해 사용자 PC를 네트워크에 접속할 수 있다.



[그림 1-19] 사용자 단말기의 무선 접속을 위한 와이파이 네트워크 구현

(나) 와이파이 AP를 통해 클라이언트 네트워크를 구성할 경우 추가 보호대책을 적용한다.

- 1) 무선 네트워크 장비 접속 단말기 인증 및 보안
- 2) 무선 네트워크 장비 (예: AP, Access Point) 보안 및 허용 장비 리스트
- 3) 무선 네트워크를 통하여 접근 할 수 있는 정보시스템 범위 정의
- 4) 무선 네트워크 사용권한 신청/변경/삭제 절차
- 5) 사용자 식별 및 인증
- 6) 무선 네트워크 서비스 거리 제한 (주파수 세기 조정)
- 7) 정보송수신 시 무선망 암호화 기준 (예: WPA2)
- 8) 전산실 등 통제구역 내 무선 네트워크 사용 제한
- 9) SSID(Service Set ID) 브로드캐스팅 중지 및 추측 어려운 SSID 사용 등

② 네트워크 보안 운영 관리체계를 설계한다.

네트워크 보안 관제 체계, 네트워크 자산정보 관리체계, 네트워크 구성 변경 등에 대한 보안성 승인절차 등을 포함하는 네트워크 보안 운영 관리체계를 수립한다.

1. 보안 자산 정보 관리 체계를 설계한다.

보안 관리의 핵심은 자산정보의 자동화된 관리체계 및 현행화 체계이다. 네트워크를 구성하는 주요 자산 목록, 구성도, IP 현황을 최신으로 유지하고 외부에 유출되지 않도록 안전하게 관리한다.

(1) 네트워크를 구성하는 주요 자산정보의 관리체계를 설계한다.

보호 대상이 되는 유형 자산에 대한 정보 관리체계를 수립한다.

(가) 서버팜 내의 주요 서버 호스트에 대한 자산정보 관리체계를 설계한다.

자동화된 정보수집체계를 기반으로 서버 호스트에 대한 IP 주소, 설치 소프트웨어 목록, 리소스 사용량에 대한 정보 관리 및 현행화 체계를 수립한다.

(나) 서버팜 내의 주요 네트워크 장비에 대한 자산정보 관리체계를 설계한다.

네트워크 장비 및 보안장비의 유형과 IP 주소에 대한 자산정보 관리체계 및 현행화 체계를 수립한다.

<표 1-23> 정보자산 관리 정책의 예시

구분	목적	세부정책
정보자산 식별	조직의 업무특성에 따라 정보자산 분류기준을 수립하고 정보보호 관리체계 범위 내 모든 정보자산을 식별하여야 한다. 또 식별된 정보자산을 목록으로 관리하여야 한다.	정보자산(정보시스템, 정보보호시스템, 정보)의 분류기준을 수립하고 정보보호 관리체계 범위 내 모든 정보자산을 식별한다.
		식별된 정보자산을 다음 항목이 포함된 별도 목록으로 관리한다.
		-정보자산명, 자산번호, 모델명, 용도
		-정보자산별 책임자, 관리자, 관리부서
보안등급 과 취급	기밀성, 무결성, 가용성, 법적 요구사항 등을 고려하여 정보자산이 조직에 미치는 중요도를 평가하고 그 중요도에 따라 보안등급을 부여하여야 한다. 또 보안등급을 표시하고 등급 부여에 따른 취급절차를 정의하여 이행하여야 한다.	-정보자산에 대한 보안등급 등
		정기적으로 정보자산 현황을 조사하고 정보 자산목록을 최신으로 유지한다.
		식별된 정보자산에 대한 책임자 및 관리자(또는 담당자)를 지정한다.
		기밀성, 무결성, 가용성, 법적 요구사항 등을 고려하여 정보자산의 중요도를 평가하기 위한 기준을 수립한다.
		정보자산별로 중요도를 평가하고 각 자산별 특성에 적합한 보안등급 부여한다.
		정보자산의 보안등급에 따른 취급절차(생성, 저장, 이용, 파기 등)를 정의하고 이행한다.

(2) 보안 관리가 필요한 기타 자산정보의 관리체계를 설계한다.

보호 대상이 되는 무형 자산에 대한 정보관리 체계를 수립한다.

(가) 조직에서 운영 중인 웹사이트 정보에 대한 관리체계를 설계한다.

도메인 네임 서비스의 등록 요청 및 승인 체계와 연계한 웹사이트 정보의 관리체계 및 현행화 체계를 설계한다.

(나) 조직에서 운영 중인 API 정보에 대한 관리체계를 설계한다.

웹 브라우저에서 직접적으로 호출되지 않지만, 타 서버 혹은 모바일 앱의 서비스를 위해 외부에 오픈되는 API 정보에 대한 관리체계 및 현행화 체계를 설계한다.

## 2. 네트워크 보안 관제 체계를 설계한다.

네트워크 보안장비에서 발생하는 다양한 이벤트 및 로그 정보와 이를 통합적으로 수집 제공해주는 ESM 솔루션 등을 활용한 네트워크 보안관제 체계를 설계한다.

(1) 네트워크 보안관제 대상을 정의한다.

(가) 보안 자산 정보를 기반으로 하여 보안 관제 대상이 되는 네트워크와 시스템을 선정한다.

(나) 이벤트 혹은 보안 침해사고 발생 시 경보를 전달할 수신자를 정의한다.

(2) 보안 이벤트 탐지 및 분석 방법을 정의한다.

(가) 보안 이벤트의 수집 및 통합 로그 분석 방법을 정의한다.

(나) 로그 통합 분석을 통한 보안 이벤트의 침해 판단 임계치를 정의한다.

(3) 보안 침해 대응 방안을 정의한다.

(가) 보안 이벤트가 침해 공격 정탐으로 판단될 경우에 대해, 공격 IP를 차단하는 등의 긴급 대응 방안을 정의한다.

(나) 침해 공격 차단 이후 로그 분석을 통해 침입 경로와 시스템 영향성 등을 분석하고 보안 이벤트의 침해 판단 임계치 수정, 탐지 패턴 고도화 등의 후속 조치 방안을 정의한다.

## 3. 네트워크 보안 관련 보안성 승인 절차를 설계한다.

사용자 신원을 확인하고 단말기에서 사용 가능한 IP 주소를 지정된 사용 기간 동안 사용 승인하는 IP할당 통제체계와 네트워크 구성 변경에 대한 보안성 승인절차를 설계한다.

(1) 인가된 사용자만이 네트워크에 접근할 수 있도록 IP할당 통제체계를 설계한다.

사용자의 신원 확인 후 IP 주소를 할당 승인하는 체계를 수립하고 NAC 솔루션과 연계된 네트워크 접속 승인체계를 설계한다.

(가) 사용자의 IP 할당 요청 및 승인 체계를 설계한다.

사용자의 PC에서 사용할 수 있는 IP 주소의 요청 및 승인에 대한 자동화된 체계 및 관련 시스템을 설계한다.

(나) 승인된 IP를 할당받은 PC만 네트워크에 접근되도록 하는 접속 승인 체계를 설계한다.

할당이 승인된 IP가 사용되고 필수적인 보안 SW 설치가 확인된 PC만 네트워크에 접근되도록 하는 자동화된 체계 및 관련 시스템을 설계한다.

(2) 네트워크의 구성변경에 대한 보안성 승인 절차를 설계한다.

내부 네트워크 구성변경 및 연동 변경에 따른 방화벽 작업 승인 등에 대한 보안성 승인 절차를 설계한다.

(가) 내부 네트워크 구성 변경에 대한 보안성 승인 절차를 설계한다.

서버팜 내 시스템 및 네트워크의 구성 변경에 대한 보안성 검토, 승인 절차 및 관련 시스템을 설계한다.

(나) 외부 네트워크로의 연동 변경에 대한 보안성 승인 절차를 설계한다.

외부 시스템과의 신규 연동 혹은 기존 연동 규격의 변경에 대한 보안성 검토, 승인 절차 및 관련 시스템을 설계한다.

#### 수행 tip

- 웹사이트 및 API목록과 같은 정보는 웹방화벽 등의 보안시스템에 실시간으로 반영이 되어야 적절한 관제체계가 운영가능하다.
- https 기반의 웹사이트 혹은 API URL은 웹방화벽에 인증서가 등재되어야 침해공격의 탐지 및 차단이 가능하다.

## 1-3. NW 구현 준비

### 학습 목표

- 보안성이 강화된 네트워크 구현을 위한 환경을 구축할 수 있다.
- 보안성이 강화된 네트워크 구현을 위한 일정 계획을 수립할 수 있다.

## 필요 지식 /

### ① 정보통신 네트워크 구축 절차

네트워크 구축 절차는 기본적으로 다음 4단계로 나뉘며 순환 주기는 소요 트래픽 증가량, 서비스 환경 변화에 따라 달라진다.

#### 1. 1단계 - 진단 및 분석(Analysis)

- (1) 제공 서비스에 대한 요구사항 분석
- (2) 기존 네트워크에 대한 기술적 분석을 통해 기본 품질 목표 결정
- (3) 다양한 제약사항에 의한 최종 품질 목표 도출

#### 2. 2단계 - 설계(Design)

- (1) 진단 및 분석단계에서 도출된 품질 목표 만족을 위한 네트워크 구축 목표와 원칙 수립
- (2) 네트워크 아키텍처 설계 및 구간별 네트워크 대역폭에 대한 장비 용량 산정
- (3) 아키텍처 및 장비 용량을 충족하는 네트워크 장비와 솔루션 선정
- (4) 선정된 네트워크 장비에 대한 구축 일정 계획 수립

#### 3. 3단계 - 설치/구축(Implementation)

- (1) 설계 결과와 일정 계획에 따른 네트워크 장비 구축
- (2) 네트워크 구축 결과가 서비스 요구사항과 품질 목표를 만족하는지 검증

#### 4. 4단계 - 운용(Operation)

- (1) 네트워크 운용 수행
- (2) 네트워크 품질 기준 목표 유지 여부 관리
- (3) 차기 네트워크 고도화에 대한 진단 분석 단계의 기초자료로 활용할 수 있도록 운용 품질 지표 수집 관리

## ② 정보통신 네트워크 설계 개요 및 세부 요건

### 1. 네트워크 설계 개요

#### (1) 네트워크 설계 업무

네트워크의 신규 구축, 장비 대개체 및 증설, 구조 변경 등에 대해 계획을 세우고 설계 도면 및 내역서 등을 작성하는 과정을 포함한다.

#### (2) 네트워크 설계 목적

네트워크 노드 간 상호 통신이라는 기능적 요구사항과 가용성, 속도, 저지연 등 품질 특성과 관계되는 비기능적 요구사항을 충족하기 위한 것이다.

### 2. 네트워크 설계의 요건

#### (1) 경제성

투자비용 대비 정량적 및 정성적 효과를 고려한다.

#### (2) 가용성

일부 노드의 장애가 발생하더라도 전체 서비스 중단이 발생하지 않도록 이중화 등을 고려한다.

#### (3) 확장성

네트워크 구축 이후 네트워크 장비, 운용 관리 시스템 등의 확장 혹은 변경이 용이하도록 기술 호환성을 고려한다.

#### (4) 운용 효율성

네트워크 운용 단계의 운영 편의성, 업무 효율성, 대응 용이성 등 운영 관리 효율성을 고려한다.



## 수행 내용 / NW 구현 준비하기

### 재료 · 자료

- 정보통신망 이용촉진 및 정보보호 등에 관한 법률
- 개인정보 보호법
- 정보보호관리체계에 관한 국제 표준 규격(ISO27001)
- 정보보호관리체계(ISMS) 인증기준 세부 점검항목
- 개인정보보호관리체계(PIMS) 인증기준 세부 점검항목

### 기기(장비 · 공구)

- 인터넷
- 컴퓨터
- 프린터
- 문서 작성 도구

### 안전 · 유의 사항

- 각종 규제 기준과 가이드를 통해 도출된 보안 요구사항을 준수할 수 있도록 네트워크 보안 설계를 순차적으로 진행한다.
- 네트워크 보안 체계의 기반이 되는 정보통신 기본 네트워크를 설계하고 보안 구현의 단계별 일정 계획을 수립한다.

### 수행 순서

#### ① 네트워크 보안 구현을 위한 정보통신 기본 네트워크를 설계한다.

1. 가용성을 고려하여 네트워크 보안 구현을 위한 기본 네트워크를 설계한다.
  - (1) 백본 라우터 하위의 네트워크 장비 구성을 설계한다.
  - (2) 계층별 주요 네트워크 장비를 주장비와 이중화 장비로 구분하고, 완전 그물망(Full Mesh) 형태로 구성한다.
  - (3) 계층별 주요 네트워크 장비는 링크 장애 대비를 위해 인터링크 네트워크를 구성한다.
  - (4) 완전 그물망 네트워크의 루프 현상을 방지하기 위해 STP(Spanning Tree Protocol) 등 적절한 설정을 적용한다.

2. 서비스 요구사항을 고려하여 네트워크 장비와 회선의 용량을 설계한다.

(1) 서비스 네트워크 예상 가입회선 수를 상정한다.

(2) 예상 가입회선 수와 회선별 평균 트래픽 수치를 곱하여 네트워크 용량을 도출하고 용량 마진을 추가로 고려한다.

## ② 네트워크 보안 구현을 위한 일정 계획을 수립한다.

1. 네트워크 보안 구현을 위한 일정 계획을 수립한다.

세부 업무 과제를 정의하고 과제별 우선순위에 따른 구현 일정계획을 수립한다.

(1) 네트워크 기본 구성 및 네트워크 보안 설계의 주요 세부 업무를 정의한다.

네트워크 장비와 보안 장비 및 솔루션 구축을 위한 세부 업무단위를 구분하여 정의한다.

(2) 정의된 세부업무에 대한 우선순위를 정의한다.

도출된 세부 업무 단위별로 과업의 긴급도와 중요도를 고려하여 우선순위를 정의한다.

2. 세부 업무 단위별 일정 계획을 수립한다.

과업에 따라 연차별 계획과 당해 연도 일정 계획을 수립한다.

(1) 네트워크 구축 및 보안 설계에 대한 연차별 계획을 수립한다.

전체 네트워크 보안 설계 범위에 대한 마스터 플랜을 수립한 이후에는 연차별로 진행해야 하는 일정 계획을 수립한다. 과업의 긴급도와 중요도를 기반으로 우선순위를 수립한 이후 연차별 계획을 수립 시에는 연차별로 투입 가능한 예산이 중요 고려 요소이다.

(2) 네트워크 구축 및 보안 설계에 대한 당해 연도 일정 계획을 수립한다.

당해 연도에 구축할 네트워크 구축 및 증설, 보안 솔루션 구축과 관련하여 일정 계획을 수립하되, 과업 간의 의존 관계를 고려하여 일정 계획을 수립해야 한다.

### 수행 tip

- 일정 계획을 수립할 때 위험분석 방법론을 사용하여 긴급도와 중요도, 가용예산을 고려하여 순차적으로 진행되도록 유의한다.

**교수 방법**

- 정보통신망법과 개인정보 보호법에 근거한 네트워크 보안 요구사항에 대한 학습자의 지식 보유 수준을 확인하고, 주요 사항을 간단히 설명한다.
- 정보보안 침해 공격 방법과 이의 대응을 위한 주요 보안장비에 대한 학습자의 지식 보유 수준을 확인하고, 주요 사항을 간단히 설명한다.
- 네트워크 보안 설계의 기본 원칙에 대해 사례를 들어 설명한다.
- 법적 망분리 대상 기준에 대한 학습자의 지식 보유 수준을 확인하고, 망분리 요건의 준수를 위한 네트워크 보안 설계 방법에 대해 유형별로 설명한다.
- 무선 AP의 보안 설계를 위한 유의사항과 기술적인 보호대책을 상세히 설명한다.
- 네트워크 보안 운영관리를 위한 자산정보 관리체계와 보안성 승인절차의 취지와 함께 구체적인 절차에 대해 설명한다.

**학습 방법**

- 정보통신망법과 개인정보 보호법에 근거한 네트워크 보안 요구사항에 대한 내용을 되뇌어 보고, 주요 내용을 노트에 정리한다.
- 정보보안 침해 공격 방법과 이의 대응을 위한 주요 보안장비에 내용을 되뇌어보고, 주요 내용을 노트에 정리한다.
- 네트워크 보안 설계의 기본 원칙을 사례와 함께 숙지한다.
- 법적 망분리 대상 기준에 대한 내용을 되뇌어보고, 망분리 요건의 준수를 위한 네트워크 보안 설계 방법에 대해 유형별로 숙지한다.
- 무선 AP의 보안 설계를 위한 유의사항과 기술적인 보호대책을 상세히 확인한다.
- 네트워크 보안 운영관리를 위한 자산정보 관리체계와 보안성 승인절차의 취지와 함께 구체적인 절차에 대해 숙지한다.

## 평가 준거

- 평가자는 학습자가 학습 목표를 성공적으로 달성하였는지를 평가해야 한다.
- 평가자는 다음 사항을 평가해야 한다.

학습 내용	학습 목표	성취수준		
		상	중	하
NW보안 요구사항 명세	- 정의된 보안요구사항에 따라 네트워크에 대한 보안 요구사항을 명세할 수 있다.			
NW보안 설계	- 명세된 보안 요구사항을 만족하는 네트워크를 설계할 수 있다.			
NW 구현 준비	- 보안성이 강화된 네트워크 구현을 위한 환경을 구축할 수 있다.			
	- 보안성이 강화된 네트워크 구현을 위한 일정 계획을 수립할 수 있다.			

## 평가 방법

- 문제해결 시나리오

학습 내용	평가 항목	성취수준		
		상	중	하
NW보안 요구사항 명세	- 정의된 보안요구사항에 따라 네트워크에 대한 보안 요구사항을 명세하는 과정의 적정성 여부			
NW보안 설계	- 명세된 보안 요구사항을 만족하는 네트워크를 설계하는 과정의 적정성 여부			
NW 구현 준비	- 보안성이 강화된 네트워크 구현을 위한 환경을 구축하는 과정의 적정성 여부			
	- 보안성이 강화된 네트워크 구현을 위한 일정 계획을 수립하는 과정의 적정성 여부			

• 서술형 시험

학습 내용	평가 항목	성취수준		
		상	중	하
NW보안 요구사항 명세	- 정보통신망법 및 개인정보 보호법의 규제 유형과 각종 보안침해사고 유형 및 보안 장비의 유형에 대한 기본 지식			
NW보안 설계	- 명세된 보안 요구사항을 만족하는 네트워크를 설계하기 위한 네트워크 설계 원칙 및 설계 사항에 대한 기본 지식			
NW 구현 준비	- 가용성이 확보되는 기본 네트워크 구현을 위한 기본 지식			
	- 네트워크 구현 일정 계획을 수립할 때 고려해야 할 요소에 대한 기본지식			

## 피드백

### 1. 문제해결 시나리오

- 네트워크 보안 요구사항의 도출을 위한 법적 근거와 함께, 요구사항명세 및 네트워크 보안 설계를 수행하는 과정의 시나리오 전개상 부족한 부분을 지적하고 개선이 가능한 부분을 피드백한다.

### 2. 서술형 시험

- 네트워크 보안 설계 요구사항 도출에 필요한 각종 법률 규제 사항, 보안위협 종류 및 보안장비의 유형, 보안 설계의 기본 원칙과 보안 설계 수행 시의 필수 고려사항 등과 기본 지식 중 오류 사항을 피드백하여 학습자가 재학습 후 학습목표를 달성할 수 있도록 한다.

## 2-1. NW보안 구현

### 학습 목표

- 수립된 네트워크 보안 구현 계획에 따라 네트워크 보안을 구현할 수 있다.

### 필요 지식 /

#### ① 네트워크 ACL 설정

##### 1. 네트워크 ACL의 개념

###### (1) 네트워크 ACL의 정의

허가받지 않은 이용자나 트래픽이 라우터나 네트워크의 특정자원에 접근하는 것을 차단하거나 허용하는 것을 의미하며, 라우터의 인터페이스에 적용되어 사전 설정한 내역에 따라 특정 패킷을 필터링할 수 있다.

###### (2) 네트워크 ACL 적용 시 장단점

###### (가) 네트워크 ACL 적용 시 장점

라우터 내부 혹은 라우터 간에 유통되는 불필요한 트래픽을 줄임으로써 네트워크 부하를 줄일 수 있으며 네트워크 보안성이 향상된다.

###### (나) 네트워크 ACL 적용 시 단점

패킷을 검사하는 과정에서 지연이 발생하므로 과도한 ACL이 적용될 경우 라우팅 성능 저하가 유발된다.

##### 2. 네트워크 ACL의 종류

###### (1) 표준 ACL (Standard ACL)

(가) 기본적인 ACL로써 패킷의 출발지 주소만 검사하여 제어한다.

(나) ACL 번호: 1 ~ 99, 1300 ~ 1699

###### (2) 확장 ACL (Extended ACL)

(가) 패킷의 출발지 주소, 목적지 주소와 프로토콜, 포트번호 등을 검사하여 제어한다.

(나) ACL 번호: 100 ~ 199, 2000 ~ 2699

## ② 보안 운영 관리를 위한 ESM

### 1. ESM(Enterprise Security Management)의 개요

#### (1) ESM의 개념

네트워크에 유입되는 다양한 위협요소들을 총체적으로 분석하여 미리 예방할 수 있도록 지원하는 솔루션이다.

#### (2) ESM의 주요 기능

##### (가) 보안 이벤트 수집 및 가공

에이전트를 통한 각종 보안 이벤트를 수집하고 가공(정규화, 필터링, 축약 등)한다.

##### (나) 보안 이벤트 통합 관리

수집된 이벤트를 단일 장비 내 분석, 이종 보안장비 간 연계 분석하며, 콘솔에서 실시간 모니터링하도록 지원한다.

##### (다) 침해 경보

보안 침해 징후 발견 시 침해 징후 수준에 따라 경보 수위를 달리하여, 가시/가청/메일/메시징 형태로 경보를 발령한다.

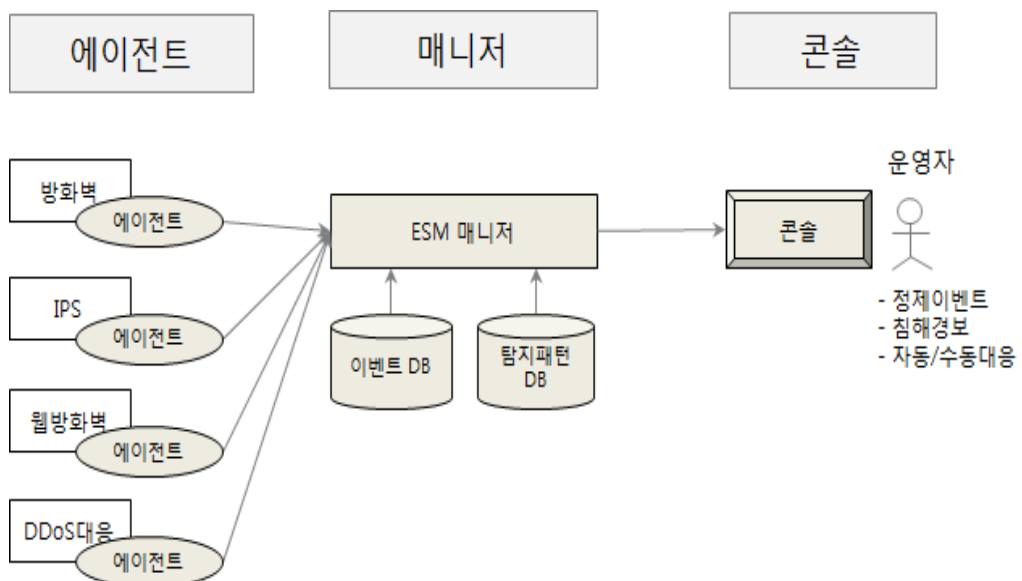
##### (라) 침해 대응

침해 상황별로 ESM의 자동대응 혹은 운영자의 수동대응을 지원하며 침해사고와 관련된 증거와 로그를 보관한다.

### 2. ESM의 구성

#### (1) ESM의 구성도

ESM은 이벤트 수집 에이전트와 매니저, 관리 콘솔로 구성된다.



[그림 2-1] ESM의 구성도

## (2) ESM의 구성 요소별 주요 기능

### (가) ESM 에이전트

보안장비, 시스템장비, 네트워크 장비 등에 탑재되어 사전에 정의된 규칙에 의해 이벤트를 수집하여 매니저로 전달하거나 보안정책을 반영한다.

### (나) ESM 매니저

사전에 정의된 규칙에 의해 이벤트 데이터 분석하고 저장하며, 정제된 이벤트를 콘솔로 전달한다.

### (다) ESM 콘솔

매니저에 의해 전달된 자료의 시각적 정보를 화면을 통해 제공하여, 운영자 판단을 지원하며, 침해 발생 시 경보를 발령하고 자동 혹은 수동 대응을 지원한다.

## 3. ESM 기반의 보안관제 업무

### (1) 보안관제 업무의 정의

보안관제는 외부 위협의 침입 가능 경로를 모니터링하고 이벤트를 감지하여 침해 사고를 예방하는 활동을 의미한다.

<표 2-1> 보안관제 업무의 주요 역할

구분	역할
보안 시스템 통합관리	서로 다른 보안 장비에 대한 ESM를 통한 모니터링 및 통합 관리
일관성 있는 정책구현	일관된 정책적용 및 중앙관리로 보안장비의 위협 요소를 최소화
신속한 대응처리	침해사고에 대한 사전 예방 활동 강화 (24X365일 실시간 감시) 및 장애 처리, 업무중단에 대한 위협 대응



## (2) 보안관제의 단계별 활동

보안관제는 사전 예방 활동, 탐지 활동, 대응 활동으로 구성된다.

<표 2-2> 보안관제의 단계별 활동

구분	활동	내용
예방 단계	보안 취약점 패치	서버, 네트워크 장비, 응용 프로그램 등에서 식별된 보안취약점을 패치를 적용하여 제거함
	취약점 점검	시스템 및 네트워크 장비에 대해 주기적으로 취약점을 점검하고 조치함
	정책 관리	IDS, IPS, 방화벽, 네트워크 장비 등에 보안정책을 적용함
	모니터링	이벤트 로그, 시스템 로그 등 각종 이벤트에 대해 확인함
탐지 단계	NMS, Alert	네트워크 및 시스템에서 제공하는 예경보를 탐지함
	시스템 장애 이벤트	각종 시스템 장애에서 발생하는 경보에 대해 탐지함
	관리적 이벤트	기타 관리에 필요한 각종 이벤트에 대해 탐지함
대응 단계	웜·바이러스	웜, 바이러스, 백도어, 악성 봇 등 악의적인 프로그램 감염에 대해 대응함
	스캐닝	악의적인 의도로 시설에 관련된 정보 수집하는 활동에 대해 대응함
	침해사고	주요 시스템에 불법적인 접근을 시도하고 권한을 획득하는 활동에 대해 대응함
	기타 사고대응	기타의 다양한 정상, 비정상적인 이벤트 및 활동에 대해 대응함(사이버 시위 등)

## 수행 내용 / NW보안 구현하기

### 재료 · 자료

- 정보통신망 이용촉진 및 정보보호 등에 관한 법률
- 개인정보 보호법
- 정보보호관리체계에 관한 국제 표준 규격(ISO27001)
- 정보보호관리체계(ISMS) 인증기준 세부 점검항목
- 개인정보보호관리체계(PIMS) 인증기준 세부 점검항목

### 기기(장비 · 공구)

- 인터넷
- 컴퓨터
- 프린터
- 문서 작성 도구

### 안전 · 유의 사항

- 네트워크 보안 설계 항목을 수립된 일정 계획에 맞게 구현한다.
- 관문 네트워크 보안 체계, 서버 네트워크 분리, 클라이언트 네트워크 접근 통제 체계 및 보안 운영 관리 시스템을 구축하고 보안설정을 수행한다.

### 수행 순서

① 네트워크 장비 및 네트워크 보안 장비를 구성하고 보안항목을 설정한다.

1. 네트워크 장비 및 네트워크 보안 장비를 배치하고 기본 설정을 적용한다.

- (1) 네트워크 설계에 따라 라우터 및 스위치 등의 네트워크 장비를 설치한다.
- (2) 네트워크 설계에 따라 방화벽, IPS, 웹방화벽, DDoS대응 장비 등의 네트워크 보안 장비를 설치한다.
- (3) 네트워크 장비의 인터페이스별로 Duplex 및 전송 속도 설정을 수행한다.
- (4) 네트워크 장비별로 사전 설계에 따른 IP 주소 대역 정보 및 라우팅 테이블 정보를 인터페이스에 설정하고 관리 인터페이스의 IP 주소를 설정한다.
- (5) 네트워크 장비 인터페이스별로 정상 통신 여부에 대한 기본 시험을 수행한다.

## 2. 네트워크 장비의 보안 관련 항목을 설정한다.

### (1) 라우터 및 스위치에 대한 보안 설정을 수행한다.

#### (가) 라우터 및 스위치의 접근 통제 설정을 수행한다.

콘솔 포트를 사용한 원격 접속 시에 인증을 수행하도록, 관리자에 대한 계정과 패스워드를 설정한다.

#### (나) 불필요한 서비스와 프로토콜을 비활성화한다.

ICMP나 finger, http, CDP, bootp, dns 등 서비스에 불필요한 서비스와 프로토콜을 비활성화한다.

<표 2-3> 라우터에서 차단해야 하는 서비스 목록의 예시

포트	서비스
1 (TCP & UDP)	tcpmux
7 (TCP & UDP)	echo
9 (TCP & UDP)	discard
11 (TCP)	systat
13 (TCP & UDP)	daytime
15 (TCP)	netstat
19 (TCP & UDP)	chargen
37 (TCP & UDP)	time
43 (TCP)	whois
67 (UDP)	bootp
69 (UDP)	tftp
93 (TCP)	supdup

#### (다) NTP를 활용하여 시간 동기화 설정을 수행한다.

정확한 로그 분석을 위해 시간 동기화 서버를 통해 주기적으로 시간이 동기화되도록 설정한다.

#### 라우터의 NTP 설정 예시

```
Router (config) #ntp server 129.237.32.2
Router (config) #^Z
```

(2) 라우터 및 스위치를 이용한 네트워크 보안 설정을 수행한다.

(가) 인터페이스별로 접근통제 목록(ACL, Access Control List)을 설정한다.

라우터나 스위치의 인터페이스별로 패킷을 통과시키거나 차단하도록 접근통제 목록을 설정한다.

(나) ingress/egress 필터링을 설정한다.

사용하지 않는 대역에서 인입되는 IP 대역을 차단하고(ingress filtering), 라우터 내부에서 외부로 나가는 패킷의 소스 IP가 라우터 내부 IP인 것만 허용하도록(egress filtering) 설정한다.

3. 서버 네트워크 영역의 보안 장비 및 솔루션을 구성하고 보안 관련 항목을 설정한다.

(1) 방화벽 장비에 대한 보안 설정을 수행한다.

(가) 인터넷 관문 방화벽에 대해 보안 설정을 수행한다.

사전에 허용 또는 차단하도록 지정된 네트워크 대역 혹은 IP 주소별로 접근 허용 혹은 차단 설정을 수행한다.

(나) 영역 분리 방화벽에 대해 보안 설정을 수행한다.

DMZ와 내부망, 내부망과 폐쇄망, 운영망과 개발망 등의 영역을 분리하는 방화벽에 대해 사전에 허용 또는 차단하도록 지정된 네트워크 대역 혹은 IP 주소별로 접근 허용 혹은 차단 설정을 수행하고, 공인 IP 주소와 사설 IP 주소 간의 주소 변환(NAT, Network Address Translation) 기능을 설정한다.

(2) IPS 및 기타 네트워크 보안 장비의 보안설정을 수행한다.

(가) IPS장비에 대해 탐지 패턴 및 임계치 설정을 수행한다.

침입 탐지 패턴과 탐지 임계치를 설정하고 탐지 혹은 차단 적용 등 세부 운영 정책 사항을 정의하고 설정한다.

(나) 웹방화벽 장비에 대해 탐지 패턴을 정의하고 설정을 수행한다.

SQL 삽입 공격이나 XSS 등 주요 웹 공격에 대한 공격 패턴을 정의하고 이에 대해 탐지 및 차단 여부를 설정한다.

(다) DDoS 대응 장비에 대해 탐지 패턴을 정의하고 설정을 수행한다.

비인증 혹은 비정상 트래픽에 대한 패턴 및 탐지 임계치를 설정하고 이에 대한 탐지, 방어 및 경보 방법에 대한 설정을 수행한다.

(라) 악성코드 유입방지 솔루션에 대해 보안 설정을 수행한다.

APT 혹은 기타 경로를 통해 유입되는 악성코드를 탐지하기 위한 패턴을 설정하고, 클라우드를 통해 관리되는 악성코드 DB와 실시간 연동되도록 보안설정을 수행한다.

(마) VPN 솔루션에 대한 설정을 수행한다.

외부에서의 불가피한 원격 접속을 지원할 수 있는 SSL VPN 접속을 위한 계정관리 및 인증 시스템, 2차 인증 방식 등에 대한 설정을 수행한다.

(바) ESM 솔루션에 대한 설정을 수행한다.

분석 대상 보안 장비에 설치되는 Agent, 수집서버, DB서버 및 분석서버 등에 대한 환경 설정을 수행한다.

#### 4. 클라이언트 네트워크 영역의 보안 장비 및 솔루션을 구성하고 보안 관련 항목을 설정한다.

(1) 클라이언트 PC와 기기의 네트워크 접근통제를 위한 NAC 솔루션을 구성하고 보안 관련 항목을 설정한다.

클라이언트 PC의 식별 및 인증 방식, 네트워크 접근통제 유형, 비인가 단말의 격리 방식 등에 대한 보안설정을 수행한다.

(2) 클라이언트 PC의 인터넷 및 업무망 분리를 위한 망분리 솔루션을 구성하고 보안 관련 항목을 설정한다.

망분리 대상자에 대한 인터넷 차단 자동 적용 설정, 망분리 솔루션 특성에 따른 매체 제어 설정(호스트 기반 망분리 적용자 대상), 망간 자료 전송 방식 및 승인 체계 등 연관 항목에 대한 보안 설정을 수행한다.

(3) 클라이언트 PC의 와이파이 네트워크 접속을 위한 무선망 장비 및 솔루션을 구성하고 보안 관련 항목을 설정한다.

AP 접속 및 사용자 인증방식, wifi 망 내 데이터 전송 암호화 방식, SSID Broadcast 여부 등 와이파이 AP의 보안 관련 항목을 설정한다.

### ② 네트워크 보안 운영을 위한 업무 처리 시스템을 구성한다.

#### 1. 네트워크 보안 자산 정보의 관리체계 운영을 위한 시스템을 구성한다.

(1) 네트워크 보안 관련 주요 자산 정보의 관리체계 운영을 위한 시스템을 구성한다.

(가) 데이터 센터 내 주요 실물 서버 혹은 가상화 서버 호스트에 대한 자산정보 수집 및 현행화 관리 시스템을 구축한다.

(나) 데이터 센터 내 주요 네트워크 장비 및 네트워크 보안 장비에 대한 자산정보 관리 시스템을 구축한다.

(2) 보안관리가 필요한 기타 자산정보의 관리체계 운영을 위한 시스템을 구성한다.

(가) 기관에서 운영 중인 웹사이트 정보를 관리하기 위한 관리시스템을 구축한다.

(나) 기관에서 운영 중인 오픈 API 정보를 관리하기 위한 관리시스템을 구축한다.

(다) 웹사이트와 오픈 API 정보의 지속적인 현행화를 위해 DNS 서버 및 DNS 정보 관리 서버와의 정보 갱신 체계를 구축한다.

## 2. 네트워크 보안 형상 변경에 대한 보안성 승인절차 운영을 위한 시스템을 구성한다.

### (1) 인가된 사용자만이 네트워크에 접근할 수 있는 IP할당 통제체계를 구축한다.

사용자의 신원 확인 후 IP 주소를 할당 승인하는 체계를 수립하고 NAC 솔루션과 연계된 네트워크 접속 승인체계를 구축한다.

#### (가) 사용자의 IP할당 요청 및 승인 시스템을 구축한다.

사용자의 PC에서 사용할 수 있는 IP 주소의 요청 및 승인기능이 포함된 IP할당 관리시스템을 구축한다.

#### (나) 승인된 IP를 할당받은 PC만 네트워크에 접근되도록 IP할당 시스템과 NAC시스템을 연동 구현한다.

할당이 승인된 IP 주소를 가진 PC만이 네트워크에 접속될 수 있도록 IP할당 시스템과 NAC시스템의 연동을 구현한다.

### (2) 네트워크의 구성변경에 대한 보안성 승인 및 작업관리 시스템을 구축한다.

내부 네트워크 구성변경 및 연동 변경에 따른 방화벽 작업 승인 등에 대한 보안성 승인절차가 진행되는 보안성 승인시스템 및 작업관리 시스템을 구축한다.

#### (가) 네트워크 구성 변경에 대한 보안성 승인시스템을 구축한다.

서버팜 내 시스템 및 네트워크의 구성 변경에 대한 보안성 검토, 승인 절차를 구현한 보안성 승인시스템을 구축한다.

#### (나) 승인된 네트워크 구성 변경을 관리하기 위한 작업관리시스템을 구축한다.

작업계획관리 및 작업 승인 등의 업무프로세스를 관리하기 위한 작업관리 시스템을 구축한다.

## 2-2. NW보안 테스트

**학습 목표** • 네트워크 보안 구현 결과에 대하여 테스트하고 테스트 결과를 관리할 수 있다.

### 필요 지식 /

#### ① 테스트 개요

##### 1. 테스트의 일반적인 절차

###### (1) 테스트 기획

###### (가) 테스트 계획 수립

테스트의 요구사항을 수집하고, 테스트 계획을 수립하여 테스트 계획서를 작성한다.

###### (나) 테스트 케이스 작성

테스트 항목별 테스트 케이스를 작성하고 테스트 데이터를 확보한다.

###### (2) 테스트 수행

###### (가) 테스트 실행 및 측정

테스트 환경을 구축하고, 테스트를 수행하여 결과를 도출하고 데이터를 측정한다.

###### (나) 테스트 결과 분석 및 보고

측정 데이터를 분석하여, 결함 항목을 도출하고, 테스트 결과서를 작성하여 보고한다.

###### (3) 결함관리

###### (가) 결함관리 계획 수립

테스트에서 도출된 결함에 대해 조치 방법 및 일정이 포함된 결함 조치 계획을 수립한다. 결함 조치 계획에는 서비스 오픈 전 필수적으로 조치되어야 하는 핵심 결함과 그 외 결함을 구분하여 별도의 일정 계획이 수립되어야 한다.

###### (나) 결함 재조치 및 이행관리

수립된 결함 조치 계획에 따라 결함을 수정 조치한 후 다시 테스트하고, 서비스 오픈 이후 개선이 가능한 시간이 소요되는 항목에 대해서는 결함관리 계획에 따라 이행관리를 수행한다.

## 2. 테스트 계획 수립 단계의 세부 업무

### (1) 테스트 범위 정의

테스트를 수행할 범위를 정의하고, 제외영역이 있을 경우 사유를 기술한다.

### (2) 테스트 착수 및 완료 기준 정의

테스트를 시작하기 전에 완료되어야 할 선행 업무와 테스트 종료 조건을 정의한다.

### (3) 테스트 환경 및 소요 자원 정의

테스트를 수행할 하드웨어 및 소프트웨어 환경 및 인력을 포함한 소요 자원을 정의하고, 테스트 데이터 관련 사항을 정의한다.

### (4) 일정 정의

테스트의 전체 시작, 종료 일정과 함께 테스트 단계별 과업에 대한 세부 일정을 정의한다.

### (5) 기타 사항 정의

테스트 수행 시 고려사항과 위험 요소를 정의하며, 테스트 결함 관리 방안을 정의한다.

### (6) 테스트 계획서 작성, 검토 및 승인

테스트 단계별로 상세한 테스트 계획서 및 테스트 케이스를 작성하고 품질 검수 담당자와의 협의 및 승인 절차를 통해 확정한다.

## 2 테스트 유형 및 점검 기준

### 1. 단위 테스트

단위 모듈 혹은 네트워크 단일 노드 내 기능이 요구사항에 부합되는지를 테스트하기 위한 것이다.

<표 2-4> 단위 테스트의 세부 검증 유형

구분	세부 검증 유형
인터페이스 테스트	다른 모듈과의 데이터 인터페이스에 대한 테스트
자료구조 테스트	모듈 내의 자료 구조상 오류가 있는가를 테스트
수행 경로 테스트	구조 및 루프 테스트 등에 의한 논리 경로 테스트
오류 처리 테스트	각종 오류들이 모듈에 의해 적절하게 처리되는가를 테스트
경계 테스트	오류가 발생하기 쉬운 경계 값들을 테스트 케이스를 만들어 테스트



## 2. 통합 테스트

단위 테스트 결과를 기반으로 기능 모듈 간 혹은 네트워크 노드 간 연계 기능이 요구사항에 부합되는지를 테스트하기 위한 것이다.

<표 2-5> 통합 테스트의 세부 검증 유형

구분	세부 검증 유형
하향식 테스트	시스템을 구성하는 모듈의 계층 구조에서 맨 상위의 모듈부터 시작하여 점차 하위 모듈 방향으로 통합하는 방법으로써 깊이 우선의 테스트와 넓이 우선의 테스트가 가능함
상향식 테스트	시스템을 구성하는 모듈의 계층 구조에서 최하위의 모듈부터 시작하여 점차 상위 모듈 방향으로 통합하는 방법임
혼합식 테스트	하향식 통합 전략과 상향식 통합 전략을 절충한 방식으로써 우선적으로 통합을 시도할 중요 모듈들을 선정한 후, 그 모듈을 중심으로 통합
비점진적 테스트	모든 모듈을 한꺼번에 통합하여 테스트함

## 3. 시스템 테스트

통합 테스트 결과를 기반으로 애플리케이션의 기능 요구사항이 검증된 상태에서 대상이 되는 인프라에서 실제 애플리케이션이 구동될 때에 대한 기능 검증과 함께 처리 속도 혹은 안정성 등의 비기능 요구사항을 검증하기 위한 것이다.

<표 2-6> 시스템 테스트의 세부 검증 유형

구분	세부 검증 유형
기능성	적절한 기능을 정확히 제공하고, 관련 표준을 준수하여 상호호환성이 확보되어야 하며, 정보의 접근 제한이 제공되어야함
신뢰성	결함 회피기능을 제공하고, 결함 발생 시에도 일정 성능 수준을 유지하며, 회복성이 있어야함
사용성	시스템의 사용이 편리해야 하고, 사용자가 시스템의 기능에 대한 이해와 학습이 용이해야함
효율성	적절한 반응시간과 처리율을 제공하며 효율적으로 자원을 사용해야함
유지보수성	결함의 원인 식별 및 변경이 용이해야 하고, 기능 변경 시 위험이 회피되어야함
이식성	제품의 기저 환경 변화가 용이해야 하며, 다른 제품과의 호환 및 대체가 가능해야함

#### 4. 사용자 인수 테스트

단위, 통합 및 시스템 테스트 결과를 기반으로 구현 기능이 최종 사용자의 업무 완결성 관점에서 요구사항에 부합되는지를 테스트하기 위한 것이다.

<표 2-7> 시스템 테스트의 세부 검증 유형

구분	세부 검증 유형
알파 테스트	사용자 테스트가 수행되거나 개발자 환경에서 통제된 상태로 수행
베타 테스트	개발자가 참여하지 않는 테스트로 일정 수의 시범 사용자들에 의해 수행

## 수행 내용 / NW보안 테스트하기

### 재료 · 자료

- 정보통신망 이용촉진 및 정보보호 등에 관한 법률
- 개인정보 보호법
- 정보보호관리체계에 관한 국제 표준 규격(ISO27001)
- 정보보호관리체계(ISMS) 인증기준 세부 점검항목
- 개인정보보호관리체계(PIMS) 인증기준 세부 점검항목

### 기기(장비 · 공구)

- 인터넷
- 컴퓨터
- 프린터
- 문서 작성 도구

### 안전 · 유의 사항

- 네트워크 보안 구현 항목을 검증한다.
- 네트워크 보안 구현 테스트 계획을 수립하고, 계획서에 따라 네트워크 및 네트워크 보안 구현 결과에 대한 테스트를 수행한다.

## 수행 순서

### ① 네트워크 보안 구현 테스트를 위한 테스트 계획서를 작성한다.

1. 네트워크 보안 구현의 테스트 범위 및 항목을 정의한다.
  - (1) 라우터 및 스위치 등에 대한 네트워크 기본 기능 및 성능 시험 항목을 정의한다.
  - (2) 네트워크 장비의 보안 관련 기능 시험 항목을 정의한다.
  - (3) 서버 네트워크 영역의 보안 장비 및 솔루션에 대한 기능 및 성능 시험 항목을 정의한다.
  - (4) 클라이언트 네트워크 영역의 보안 장비 및 솔루션에 대한 기능 시험 항목을 정의한다.
  - (5) 네트워크 보안 운영관리 시스템의 기능 및 성능 시험 항목을 정의한다.
2. 네트워크 보안 구현의 테스트 환경, 일정 등을 정의한다.
  - (1) 네트워크 보안 구현 테스트에 필요한 시험 환경을 정의한다.
  - (2) 테스트에 필요한 IP 주소, 테스트 데이터 등 자료 목록을 정의하고 유관부서를 통해 확보한다.
  - (3) 네트워크 보안 구현의 수행 주체와 유관 부서 대응 시험 담당자를 정의한다.
  - (4) 네트워크 보안 구현일정과 연계되는 테스트 일정을 순차적으로 정의한다.
3. 네트워크 보안 구현의 테스트 계획서를 작성한다.
  - (1) 네트워크 보안 구현 테스트를 위한 시험항목, 설정 데이터, 결함관리 방안 등이 포함된 테스트 계획서를 작성한다.
  - (2) 네트워크 보안 구현 테스트 계획서를 관련 부서 협의를 통해 검토한다.
  - (3) 네트워크 보안 구현 테스트 계획서를 확정하고 승인 절차를 진행한다.

### ② 테스트 계획서에 따라 네트워크 보안 구현 적정성을 테스트한다.

1. 라우터 및 스위치 등에 대한 네트워크 테스트를 진행한다.
  - (1) 라우터 및 스위치의 관리자 접근 통제 설정 여부를 점검한다.
  - (2) 불필요 서비스의 비활성화 여부를 점검한다.
  - (3) 타임라인 분석을 위한 시간 동기화 설정 여부를 점검한다.
2. 네트워크 장비의 보안 관련 테스트를 진행한다.
  - (1) 라우터 인터페이스별 ACL 설정 여부를 점검한다.
  - (2) Ingress/Egress 필터링 설정 여부를 점검한다.

3. 서버 네트워크 영역의 보안 장비 및 솔루션에 대한 테스트를 진행한다.
  - (1) 관문 방화벽의 IP 주소 및 포트에 대한 접근 허용 및 차단 설정 여부를 점검한다.
  - (2) 서버 영역 분리 방화벽의 접근통제 설정 및 NAT 설정 여부를 점검한다.
  - (3) IPS 장비의 탐지 패턴 적용 및 탐지 임계치 설정 여부를 점검한다.
  - (4) 웹방화벽 장비의 탐지 패턴 적용 및 관제 대상 웹사이트의 SSL인증서 등록 여부를 점검한다.
  - (5) DDoS 대응 장비의 탐지 패턴 적용 및 탐지 임계치 설정 여부를 점검한다.
  - (6) 악성코드 유입방지 솔루션의 탐지 패턴 적용 및 클라우드 DB 연동 여부를 점검한다.
  - (7) VPN 솔루션을 통한 원격 접속 성공 여부 및 로깅 동작 여부를 점검한다.
  - (8) ESM 솔루션을 통한 보안 로그 통합 수집, 임계치 기반 경고 발령, 장비 제어 여부를 점검한다.
4. 클라이언트 네트워크 영역의 보안 장비 및 솔루션에 대한 테스트를 진행한다.
  - (1) NAC 솔루션을 통한 비인가 단말의 네트워크 차단 여부를 점검한다.
  - (2) 망분리 대상자 PC의 인터넷 차단 여부 및 망간 자료 전송을 위한 결재/승인 체계 수행 동작 여부를 점검한다.
  - (3) Wifi AP 보안 설정 기준에 따른 적정 설정 여부를 점검한다.
5. 네트워크 보안 운영관리 시스템의 테스트를 진행한다.
  - (1) 네트워크 보안 관련 유/무형 자산 관리 시스템의 단위, 통합, 시스템, 인수 테스트를 진행한다.
  - (2) 사용자 IP할당 관리 시스템의 단위, 통합, 시스템, 인수 테스트를 NAC 솔루션과 연계하여 진행한다.
  - (3) 네트워크 구성 변경에 대한 보안성 승인 및 작업 관리 시스템의 단위, 통합, 시스템, 인수 테스트를 진행한다.

**교수 방법**

- 네트워크 장비의 ACL을 비롯한 보안설정 항목에 대해 학습자의 지식 보유 수준을 확인하고, 주요 사항을 간단히 설명한다.
- 서버 네트워크 관문 보안 장비 및 솔루션의 운영 목적과 함께 구체적인 설정항목에 대해 설명한다.
- 서버 네트워크 보안 관제 수행을 위한 ESM 솔루션에 대해 주요 사항을 간단히 설명한다.
- 클라이언트 네트워크의 보안 관리를 위한 NAC, 망분리, Wifi AP 보안설정에 대해 주요 사항을 간단히 설명한다.
- 네트워크 보안 운영을 위한 운영 지원 시스템의 유형과 주요 기능에 대해 간단히 설명한다.

**학습 방법**

- 네트워크 장비의 ACL을 비롯한 보안설정 항목에 대한 내용을 되뇌어보고, 주요 내용을 노트에 정리한다.
- 서버 네트워크 관문 보안 장비 및 솔루션의 운영 목적과 설정 항목을 되뇌어보고, 주요 내용을 노트에 정리한다.
- 서버 네트워크 보안 관제 수행을 위한 ESM 솔루션에 대한 내용을 되뇌어보고, 주요 내용을 노트에 정리한다.
- 클라이언트 네트워크의 보안 관리를 위한 NAC, 망분리, Wifi AP 보안설정에 대한 내용을 되뇌어보고, 주요 내용을 노트에 정리한다.
- 네트워크 보안 운영을 위한 운영 지원 시스템의 유형과 주요 기능에 대한 내용을 되뇌어보고, 주요 내용을 노트에 정리한다.

## 학습2      평      가

### 평가 준거

- 평가자는 학습자가 학습 목표를 성공적으로 달성하였는지를 평가해야 한다.
- 평가자는 다음 사항을 평가해야 한다.

학습 내용	학습 목표	성취수준		
		상	중	하
NW보안 구현	- 수립된 네트워크 보안 구현 계획에 따라 네트워크 보안을 구현할 수 있다.			
NW보안 테스트	- 네트워크 보안 구현 결과에 대하여 테스트하고 테스트 결과를 관리할 수 있다.			

### 평가 방법

- 문제해결 시나리오

학습 내용	평가 항목	성취수준		
		상	중	하
NW보안 구현	- 수립된 네트워크 보안 구현 계획에 따라 네트워크 보안을 구현하는 과정의 적정성 여부			
NW보안 테스트	- 네트워크 보안 구현 결과에 대하여 테스트하고 테스트 결과를 관리하는 과정의 적정성 여부			

- 서술형 시험

학습 내용	평가 항목	성취수준		
		상	중	하
NW보안 구현	- 수립된 네트워크 보안 구현 계획에 따라 네트워크 보안을 구현하기 위한 네트워크 장비 및 네트워크 보안장비의 보안 설정 항목에 대한 기본 지식			
NW보안 테스트	- 네트워크 보안 구현 결과에 대하여 테스트하고 테스트 결과를 관리하기 위한 절차 및 테스트 항목에 대한 기본 지식			

## 피드백

### 1. 문제해결 시나리오

- 네트워크 보안 설계에 따라 네트워크 및 네트워크 보안장비를 구축 및 설정 후 테스트를 수행하는 과정의 시나리오 전개상 부족한 부분을 지적하고 개선이 가능한 부분을 피드백한다.

### 2. 서술형 시험

- 네트워크 보안 구현에 필요한 네트워크 장비 및 네트워크 보안장비의 각종 설정 관련 지식과 운영 관리 기준에 대한 기본 지식 중 오류 사항을 피드백하여 학습자가 재학습 후 학습목표를 달성할 수 있도록 한다.

## 참고자료

---



- 한국인터넷진흥원(2003.9). 라우터 보안관리 가이드.
- 한국인터넷진흥원(2013.5). ISMS 인증기준 세부점검 항목.
- 한국인터넷진흥원(2016.11). PIMS 인증기준 세부점검 항목.



## NCS학습모듈 개발이력

발행일	2015년 12월 31일		
세분류명	보안엔지니어링(20010206)		
개발기관	(주)밸류원컨설팅, 한국직업능력개발원		
발행일	2018년 12월 31일		
학습모듈명	네트워크 보안 구축(LM2001020614_16v3)		
개발기관	(사)한국정보통신기술사협회, 한국직업능력개발원		
집필진	최상균(김포대학교)*		유두규(세명컴퓨터고등학교)
	모현철(KT)	검토진	윤용식(한국특허정보원)
	유상오(우리카드)		
	정은주(SK주)		

\*표시는 대표집필자임

## 네트워크 보안 구축(LM2001020614\_16v3)

저작권자	교육부
연구기관	한국직업능력개발원
발행일	2018. 12. 31.

※ 이 학습모듈은 자격기본법 시행령(제8조 국가직무능력표준의 활용)에 의거하여 개발하였으며, NCS통합포털사이트(<http://www.ncs.go.kr>)에서 다운로드 할 수 있습니다.



[www.ncs.go.kr](http://www.ncs.go.kr)