학교 인터넷 보안 가이드라인

초 | 중 | 고

교육부
Ministry of Education

교육부 사이버안전센터
Ministry of Education, Cyber Security Center

학교 인터넷 보안 가이드라인

초 중 고

CONTENTS

제·개정 이력

순번	제·개정일	변경내용	비 고
1	2023. 11.	· 제정	
2			
3			
4			
5			
6			
7			
8			
9			
10			

목 차

Ⅰ. 배경 및 필요성

1. 배경 04
2. 필요성 05

Ⅱ. 교육기관 네트워크 현황

1. 교육기관 네트워크 정의 06
2. 교육기관 네트워크 구조 07

Ⅲ. 업무망 보안 가이드

1. 업무망 운영 기준 08
2. 업무망 사용 시 유의점 09
   - 가. 학교 내부에 서버가 있는 경우 09
   - 나. 학교 외부에 서버가 있는 경우 11
3. 민간 클라우드서비스 사용 시 유의점 12
4. 민간 메신저 이용 시 유의점 13

Ⅳ. 교육망 보안 가이드

1. 교육망 운영 기준 14
2. 무선 공유기 계정 및 비밀번호 안내 시 주의사항 15
3. 최신 보안 업데이트 적용 17
4. 개인기기 사용 시 유의점 19
5. 유 · 무선망 혼용 사용 시 유의점 22
6. 민간 클라우드서비스 사용 시 유의점 24

[붙임] 학교 인터넷 보안 준수사항 체크리스트 27

I 배경 및 필요성

1. 배 경

본 가이드라인은 「교육부 정보보안 기본지침」 제43조(무선랜 보안)에 따라 학교장 책임하에 무선망 보안대책을 마련하게 되어 있으나, 학교에서 자체적으로 보안대책을 마련하는 데 어려움이 있어 보안대책 마련 시 본 가이드라인을 참고하도록 하여 학교의 정보보안 수준을 제고하고자 함

최근 경제 등 각 분야에서 디지털 대전환이 일어나고 있으며, 이는 교육 분야도 마찬가지이다. 학생 1인당 디지털기기 보유 대수는 **2020년에 0.2대, 2021년에 0.25대, 2022년에는 0.34대까지 가파르게 증가하는 추세이며, 이미 교사의 디지털기기 보유 대수도 2022년 교사 1인당 1.97대에 이르는 등 디지털 기반을 갖춰 나아가고 있다.**[1] 이에 따라 교사들은 태블릿 PC와 같은 디지털기기를 활용하여 온라인 수업을 진행하고, NEIS 시스템을 통해 학생들의 생활기록부를 작성하며, 교육청은 교육 행정을 온라인으로 관리하는 등 정보기술은 교육 분야에 깊이 영향을 미치고 있으며 특히, COVID-19의 영향으로 이러한 추세는 더욱 심화하였다.

이러한 교육환경에서 가장 중요하게 여겨야 하는 것은 바로 각 디지털기기를 연결해 주는 연결망인 네트워크에 대한 보안이다. 각 디지털기기와 유선과 무선으로 그물망 같이 연결된 네트워크는 온라인 교육(행정)환경에 없어서는 안 될 중요한 기반이다. 특히, COVID-19 이후로 진행하기 시작한 온라인 수업에서는 안정적인 통신망의 유지와 사용하는 기기의 보안이 가장 중요한 조건 중 하나가 되었다.

하지만 이와 동시에 네트워크는 각종 공격을 가능하게 하는 통로이기도 하다. 실시간으로 디지털기기에 쉽게 접근할 수 있다는 것은 곧 누군가의 디지털기기를 쉽게 공격할 수 있다는 의미이기도 하며 이러한 공격은 디지털기기의 활용을 어렵게 할 뿐만 아니라, 각 교육과 관련된 중요한 정보와 교사 및 학생들의 개인정보를 유출 시키는 등 다양한 문제를 발생시킨다.

1) 계보경, 곽병일, 한나라, "2022년 디지털 교육 인프라 및 학생 디지털 역량 현황", RM 2022-18, 한국교육학술정보원, 2022.

실제로 지난 3년간 발생한 전체 학교 인터넷에 대한 사이버 위협 탐지 대응 건수는 약 1.9만 건에 달할 정도로 많은 공격이 이루어지고 있다. 교육부를 비롯한 각 교육청 및 한국교육학술정보원(KERIS)에서 정보보호를 위하여 관리적 · 물리적 · 기술적 조치를 취하고 있음에도 불구하고 이러한 사고는 지속적으로 발생하고 있다.

2. 필요성

앞서 언급하였듯이 학교 인터넷에 대한 사이버 위협 탐지 대응 건수는 **최근 3년간(2019.12.~2023.05.) 약 1.9만 건에 달하고 있다,** 이러한 사이버 위협 중에서 시도교육청이 차지하는 비율이 COVID-19 이전 99%에 이를 정도로 절대적인 비율을 차지하였으나 현재에는 77.2% 정도로 감소하고 일선 학교 대상 공격 비율이 기존 1%에서 22.8%로 대폭 증가하였다.

이를 통해 이전의 서버를 보유한 시도교육청에 대한 직접 공격에서 일선 학교의 사용자를 대상으로 하는 공격으로 추세가 변경되고 있다는 것을 알 수 있다.

특히, 학교들을 대상으로 하는 사이버 위협은 곧바로 학생들의 피해(학습권, 개인정보자기결정권 등의 침해)로 연결될 수 있다.

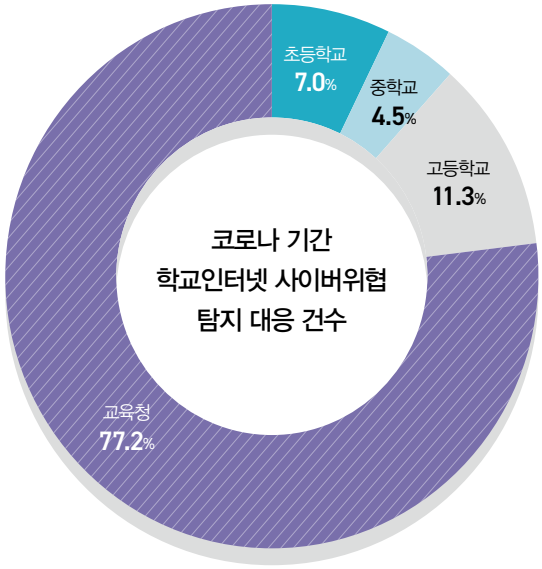

그림 1 교육부 사이버안전센터에서 최근 3년간 탐지 대응한 학교 인터넷 사이버 위협 건수 비율

사례보기

악성코드 감염

2022년 7월, ㅇㅇ고등학교 내 학생이 교사의 PC에 악성코드를 심어 해킹 후 시험지 및 답안지를 유출하여 시험을 치르다 발각된 사건이 발생

개인정보 유출

2023년 2월, ㅇㅇ고등학교 홈페이지를 통해 300여 명의 신입생 개인정보 및 내신 점수가 외부에 유출된 사건이 발생

이처럼 학교 인터넷에 대한 보안은 교육환경에서 매우 중요한 요소라 할 수 있다. 따라서 개별 시도교육청과 학교들은 학교 인터넷 보안을 위해 이하에서 언급하는 각각의 내용에 따라 안전한 교육환경을 구축할 수 있도록 최선의 노력을 다하여야 한다.

Ⅱ 교육기관 네트워크 현황

1. 교육기관 네트워크 정의

가. “유선망”이란 PC, 노트북 등이 별도의 네트워크 케이블을 통해 연결되는 네트워크를 말한다.

나. “무선망”이란 노트북, 태블릿 PC, 모바일 기기 등이 무선 액세스포인트(AP) 등을 통해 연결하는 네트워크를 말한다.

다. “스쿨넷”이란 학교와 시도교육청 및 산하기관 등에 안정된 인터넷을 제공하기 위해 전용회선으로 구축하여 운영하는 네트워크로 “업무망”과 “교육망”으로 구분된다.

라. “업무망”이란 학교에 구성된 행정업무용 네트워크로 교육정보시스템(나이스, K-에듀파인 등)에 접근할 수 있도록 유선망을 통해 구축된 네트워크를 말한다.

마. “교육망”이란 학교에서 수업 또는 학생의 교육을 목적으로 사용하는 네트워크를 말하며 교육정보시스템에 접근할 수 없고 유선망, 무선망으로 운영할 수 있다.

바. “공개 업무자료”란 업무자료 중에서 비밀 및 대외비와 비공개 업무자료를 제외한 모든 자료 또는 정보(「공공데이터의 제공 및 이용 활성화에 관한 법률」 제19조에 따라 공표된 공공데이터를 포함한다)를 말한다.

사. “비공개 업무자료”란 비밀 및 대외비를 제외한 업무자료 중에서 다음 각 목의 어느 하나에 해당하는 자료 또는 정보를 말한다.

1) 「공공기관의 정보공개에 관한 법률」 제9조 제1항에 따른 비공개 대상 정보

2) 국회 소속 공무원(「국회의원수당 등에 관한 법률」 제9조에 따른 보좌직원을 포함한다) 또는 「지방자치법」 제30조에 따른 지방의회 소속 공무원의 직무상 요구에 따라 작성 또는 취득한 자료

3) 가목에 따른 비공개 대상 정보의 주요 내용이 기술된 문장 또는 문구

그 외 본 가이드에서 사용하는 용어는 「교육부 정보보안 기본지침」을 준용한다.

2. 교육기관 네트워크 구조

현재 시도교육청과 학교에서 사용되고 있는 스쿨넷은 다음과 같이 구성되어 있다. 학교에서는 교육청의 여러 보안장비를 거친 스쿨넷 전용선으로 학교 네트워크[2]를 구축하며, 크게 업무망과 교육망으로 나누어진다.

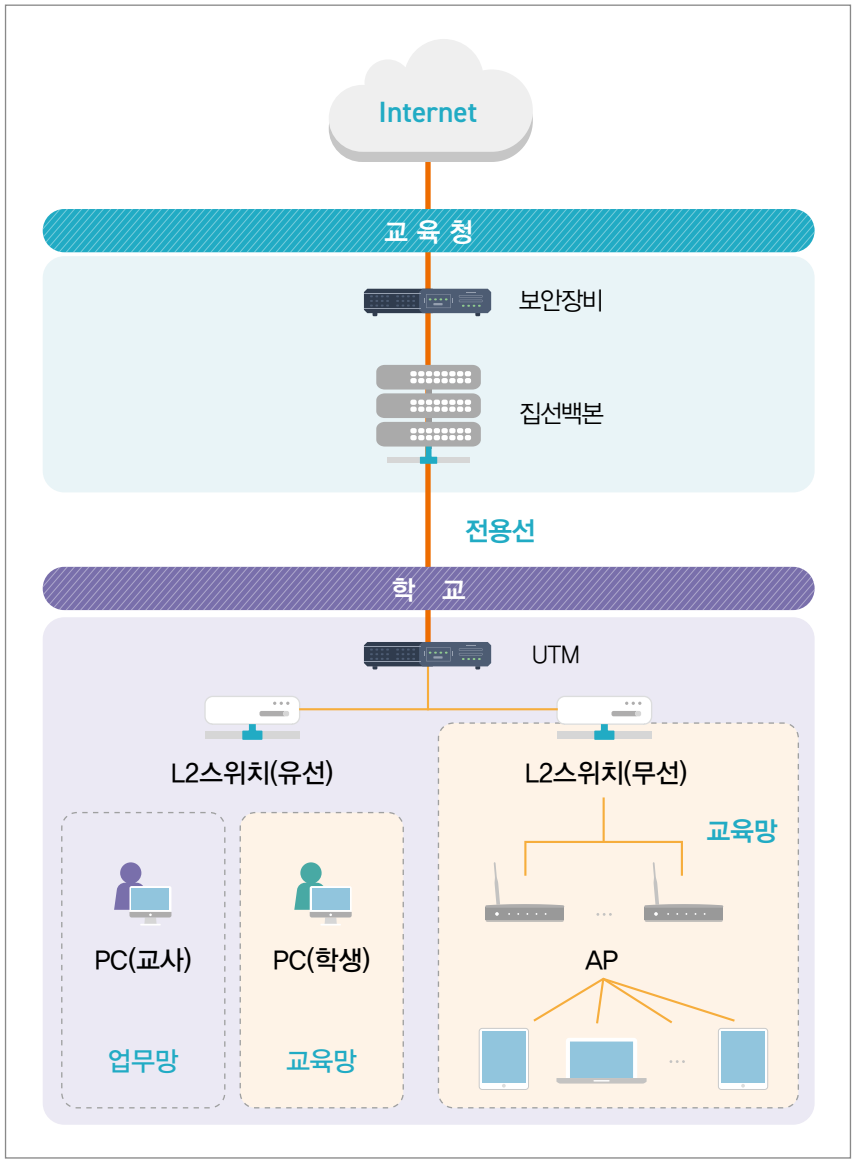

그림 2 스쿨넷 구성도

2) 네트워크 구성요소

- 보안장비 : 바이러스 및 DDoS 등 외부 공격을 차단하고, 정보유출을 방지하는 장비
- 집선백본 : 많은 트래픽을 정리해주는 네트워크 핵심 장비
- UTM(Unified Threat Management) : 여러 보안기능을 모은 통합위협관리시스템
- L2스위치 : 컴퓨터의 물리적 주소를 활용하여 케이블이 연결된 네트워크 주소(Port번호)를 찾아주는 장비
- AP(Access Point) : 무선신호를 송신하여 기기를 네트워크에 연결시키는 장비

Ⅲ 업무망 보안 가이드

1. 업무망 운영 기준

업무망이란 교육정보시스템에 접근할 수 있도록 유선망을 통해 구축된 업무용 네트워크를 말한다.
이러한 업무망의 경우 「교육부 정보보안 기본지침」에 따라 사전 승인된 단말기(PC)만 네트워크에 연결할 수 있도록 구성하여야 한다. 사전 승인된 단말기란 일정 수준의 보안 수준(최신 운영체제 및 보안패치 적용)이 적용된 단말기를 말한다.

실제 사이버 위협 탐지 시 피해확산을 방지하기 위해 교내 업무망 IP 사용 현황을 관리하며, 사이버 위협이 발생하는 경우 해당 단말기를 포맷 조치하거나 긴급 차단하는 등 보안 조치를 수행할 수 있도록 관리하여야 한다.

업무망 사용자는 본인이 PC 등 정보시스템을 사용하거나 정보통신망에 접속하는 행위와 관련하여 다음과 같이 보안을 준수하여야 한다.

보안 준수사항

- **CMOS · 로그인 비밀번호의 정기적 변경 사용 및 PC 보안관리 강화**
  업무용 PC 내 CMOS 및 로그인 비밀번호를 숫자 · 문자 · 특수문자 등을 혼합하여 안전하게 설정하여야 하며, 10분 이상 자리를 비우는 경우 화면보호기를 설정하여 재시작 시 암호를 통한 로그인을 할 수 있도록 설정
- **최신 백신 및 소프트웨어 보안패치 유지**
  PC 운영체제 및 응용프로그램에 대해 최신 보안패치를 유지하여야 하며, 파일 다운로드 시 최신 백신 소프트웨어를 통해 검사 후 활용
- **신뢰할 수 있는 사이트 및 프로그램 사용**
  의심 가는 사이트 및 출처가 불분명한 응용프로그램 사용 금지

- 인터넷 파일 공유(토렌트, 웹하드, P2P 등) · 메신저 등 업무상 불필요한 프로그램을 설치하지 아니하도록 하며, 이에 대한 지속적인 관리 필요

  업무상 부득이하게 민간 메신저를 사용해야 할 경우, 「3.4. 민간 메신저 이용 시 유의점」을 참고하여 사용 및 관리하여야 한다.

- 웹브라우저를 통해 서명되지 않은 Active-X가 다운로드 · 실행되지 않도록 보안 설정을 적용하여야 하며 다운로드 된 실행파일은 백신으로 점검 후 사용 필요

2. 업무망 사용 시 유의점

학교에서는 급식실 위생관리시스템(HACCP), 학생 출입 시 안심알리미 등 다양한 시스템을 사용하고 있으며 이러한 시스템을 사용할 때 외부 인터넷에 있는 서버를 사용하거나 학교 내부에 서버를 구축 · 운영하는 경우도 존재한다.

이러한 경우 원칙적으로 학교 네트워크를 내부망과 인터넷망으로 분리하여 인터넷망을 통해 연결을 시행하고 망연계 시스템을 통해 상호 연계를 하여야 하나 현재 학교 현장의 경우 다양한 문제로 인해 현실적으로 망 분리가 어려운 상황이다.

따라서 특별한 사유로 인해 학교 내 각 시도교육청에서 설치한 서버가 아닌 별도 시스템(민간 클라우드 포함)을 사용하는 경우 다음과 같은 보안대책을 준수하여야 한다.

가 학교 내부에 서버가 있는 경우

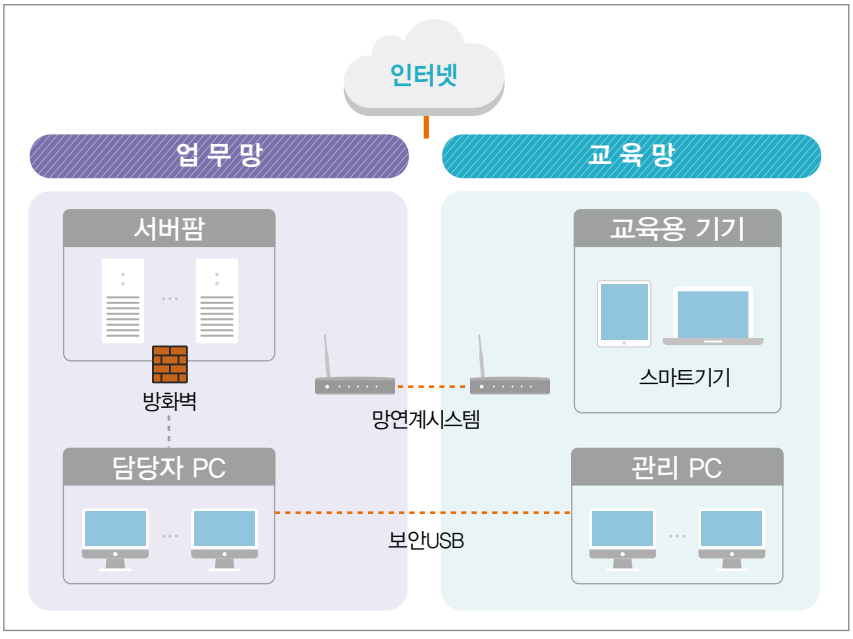

그림 3 학교 내부 서버 구성도

학교 내에 관리 서버가 있는 경우 해당 서버는 교육망이 아닌 업무망에 설치되어야 하며 이때 다음과 같은 보안을 준수하여야 한다.

❶ 서버 관리를 위한 별도의 PC를 마련하여야 하며 외부 인터넷을 통해 데이터를 주고받을 때는 망연계시스템[3] 사용 필요

❷ 학교 내 별도 망연계시스템[3]이 없는 경우 학교장 책임하에 보안 USB 사용 가능

학교 내에 별도 서버가 운영되고 있는 경우 해당 학교에서는 서버에 대한 관리자를 지정하고 보안대책을 수립하여 주기적으로 관리를 하여야 한다.

시도교육청에서는 학교 내에 설치되어 있는 서버에 대한 IP를 관리하고 보안 조치 여부를 확인하는 등 주기적인 관리 감독을 시행하고 서버 구성 및 저장되는 자료(개인정보 등)에 따라 구축 전 보안성 검토를 하여야 한다.

보안 준수사항

- 서버 관리를 위한 별도의 PC를 마련하여야 하며 외부 인터넷을 통해 데이터를 주고받을 때는 망연계시스템 사용 필요
- 학교 내 별도 망연계시스템이 없는 경우 학교장 책임하에 보안 USB 사용 가능
- 서버 운영 시 학교 내 관리자 지정 및 주기적 관리 필요
- 시도교육청은 학교 내 설치되어 있는 서버의 IP 관리, 보안 조치 확인 등 주기적 관리 감독 실시
- 학교 내 서버 설치 시 지정된 학교 내 관리자 서버 구성 및 저장자료 등을 확인하여 보안성 검토 실시

3) 망연계시스템 : 보안강화를 위해 전산망 분리를 수행했을 때 서로 분리되어 있는 전산망 간 실시간 데이터 연계와 파일 전송 기능을 제공하는 시스템

나 학교 외부에 서버가 있는 경우

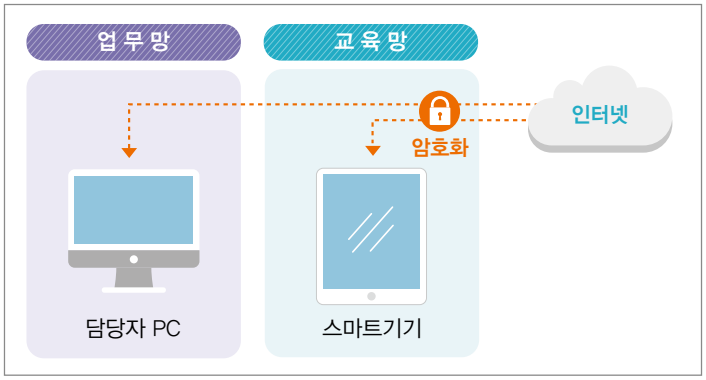

그림 4 학교 내부 서버 구성도

학교 외부에서 관리 서버가 있는 경우 해당 서버는 추가적인 보안대책을 마련하여 운영하여야 한다.
또한 민간 클라우드서비스를 이용하는 경우 「교육부 정보보안 기본지침」에 따라 국가정보원장이 게시하거나 게시 예정인 민간 클라우드서비스를 활용하여야 한다.

※ 국가사이버안보센터 – 자료실 – 지침 · 가이드 – 국가공공기관 민간클라우드컴퓨팅서비스 도입 가능 목록

외부 인터넷에 관리 서버가 있는 경우 각 학교에서는 다음과 같은 보안 수칙 적용이 필요하다.

❶ **(관리적)** 학교에서는 해당 업무용 PC에 대한 관리자를 지정하고 주기적인 보안관리 여부 점검실시
❷ **(물리적)** 업무 담당자 외 PC 임의 사용 제한
❸ **(기술적)** 해당 PC에 대한 강화된 보안정책 적용

- PC에서 접근이 가능한 시스템을 한정하고 불필요한 서비스에 접근하는 것을 차단
- 사용 시 입력 데이터, 접근범위, 데이터 암호화 여부, 서버 보안 관리 방안 등에 대한 보안성 검토 필요
- 내PC지키미, Privacy-i 등 PC 점검 도구를 사용하여 주기적인 보안 관리 실시, 이때 시도교육청에서는 관내 유사한 유형의 관리 PC에 대한 보안 정책을 별도로 수립하여 적용, 모니터링 수행 필요

※ 외부에 설치된 서버와 학교 간 전용회선을 통해 연결되어 있는 경우 학교 내 서버가 설치되어 있는 것으로 간주
※ 입력 데이터 내 개인정보가 포함되는 경우 관리용 PC와 서버 간 가상사설망(VPN)을 통해 연결 데이터를 암호화하여야 함

보안 준수사항

- 학교에서는 해당 업무용 PC에 대한 관리자를 지정하고 주기적인 보안 관리 여부 점검실시
- 업무 담당자 외 PC 임의 사용 제한
- 업무용 PC에서 접근이 가능한 시스템을 한정하고 불필요한 서비스에 접근하는 것을 차단
- 내PC지키미 등 PC 점검 도구를 사용하여 주기적인 보안관리 실시
- 사업수행 시 입력 데이터 등에 대한 보안성 검토 실시

3. 민간 클라우드서비스 이용 시 유의점

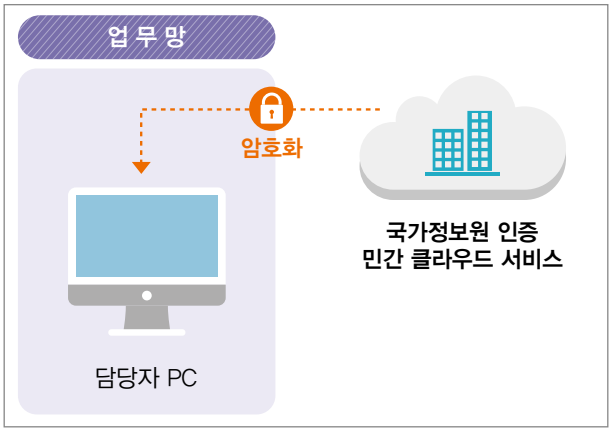

그림 5 민간 클라우드서비스 이용 시 구성도

업무망에서 민간 클라우드서비스를 활용(화상 회의 등)하여 업무를 수행하는 경우 「교육부 정보보안 기본지침」에 따라 국가정보원장이 게시한 민간 클라우드서비스를 활용하여야 한다.

※ 국가사이버안보센터 – 자료실 – 지침 · 가이드 – 국가공공기관 민간클라우드컴퓨팅서비스 도입 가능 목록

따라서, 현재 교육 현장에서 활용하고 있는 구글 문서, 마이크로소프트 365 등 민간 클라우드서비스의 경우 업무용으로는 이용할 수 없다.

또한, 민간 클라우드서비스 이용 시 서비스에 대해 네트워크 암호화(SSL 등)를 적용하고 로그인 시 2차 인증(OTP 등)을 사용하는 등 보안 조치 적용이 필요하다.

특히 개인정보를 포함하는 경우 「개인정보 보호법」에 따라 안전성 확보 조치 및 업무위탁에 따른 보호조치를 적용하여야 한다. 각급 학교 또는 시도교육청에서 교육 목적이 아닌 업무 목적을 위해 민간 클라우드를 이용하는 경우 보안성 검토를 하여야 한다.

보안 준수사항

- 구글 문서, 마이크로소프트 365 등 보안인증을 받지 않은 민간 클라우드서비스의 경우 교육용으로 용도를 한정하고 업무용으로 사용 금지
- 업무 목적을 위해 민간 클라우드 이용 시 보안성 검토 실시
  ※ 국가사이버안보센터 – 자료실 – 지침 · 가이드 – 국가공공기관 민간클라우드컴퓨팅서비스 도입 가능 목록
- 민간 클라우드서비스 사용 시 네트워크 암호화(SSL 등) 적용과 로그인 시 2차 인증 적용
- 민간 클라우드서비스 내 개인정보 포함 시 개인정보 안정성 확보 조치 및 업무위탁에 따른 보안 조치 적용 필요

4. 민간 메신저 이용 시 유의점

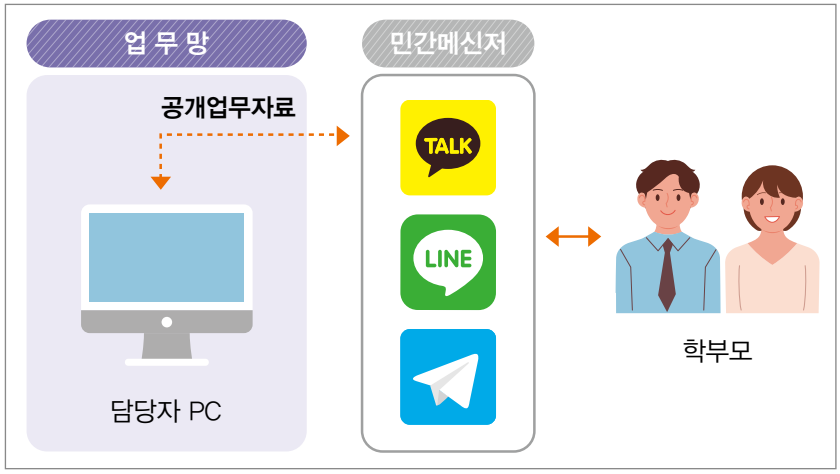

그림 6 민간 메신저 이용 시 구성도

업무망에서 민간 메신저 이용이 필요할 경우 학교장 책임하에 설치하여 사용할 수 있으며, 그 외의 경우는 설치를 금지한다.

업무상 필요에 따라 민간 메신저를 사용하는 경우 공개 업무자료만 소통하도록 주의가 필요하다.

❶ 비공개 업무자료의 경우 민간 메신저를 통해 유통되지 않도록 주의 필요
❷ 민간 메신저를 통해 자료 유통하는 경우 중요자료가 포함되지 않도록 사전 검토 필수
❸ 필요시 자료에 별도 암호를 걸어서 유통하는 등 외부 유출 방지 조치

민간 메신저를 사용 시 정기적으로 비밀번호를 변경하여 사용하며 2차 인증(OTP 등)을 적용하고 자동 로그인 기능을 비활성화하여 타인이 사용하지 못하도록 보안 조치 후 사용이 필요하다.

보안 준수사항

- 비공개 업무자료의 경우 민간 메신저를 통해 유통되지 않도록 주의
- 자료를 민간 메신저를 통해 유통하는 경우 중요자료가 포함되지 않도록 사전 검토 필수
- 필요시 자료에 별도 암호를 걸어서 유통하는 등 외부 유출 방지 조치
- 메신저 로그인 비밀번호는 정기적으로 변경하고 2차 인증 적용
- 메신저에 대한 자동 로그인 기능 비활성화

Ⅳ 교육망 보안 가이드

1. 교육망 운영 기준

교육망은 학생과 교사가 학교에서 수업 및 학생의 교육을 목적으로 사용하는 네트워크로서 최근에는 학교에서 무선 공유기를 설치하여 WiFi를 통해 다양한 모바일 기기(태블릿 PC 등), 노트북 등을 교육에 활용하는 경우가 늘어나고 있다.

이러한 교육망의 경우 관련 지침에 따라 단말기 보안, 네트워크 관리 등 관련된 보안대책을 학교장 책임하에 시행하도록 하고 있으나 학교에서 보안대책을 수립하는 데 어려움이 있어, 이에 대한 기본 사항을 다음과 같이 안내하고자 한다.

첫째, 교육망에서 유선망을 사용할 때 지정된 사설 IP를 사용하고 이에 대한 현황을 관리하여야 한다.
교육망 내에서 사용되는 IP에 대해서는 교육청에서 관내 교육망 IP 사용 현황을 관리하여 사이버 위협이 발생하는 경우 해당 PC를 포맷 조치하거나 긴급 차단하는 등 보안 조치를 수행할 수 있도록 현황을 관리하여야 한다, 다만 무선 WiFi의 경우 접속용 계정을 공용으로 사용하도록 하고 있어 별도 IP 대역으로 분리하여야 한다.

둘째, 교육망에서 업무시스템으로 접근할 수 없도록 차단 정책을 적용하여야 한다.
일선 학교에서 교육망과 업무망이 혼용되어 각각의 경계가 명확하게 설정되지 않은 경우가 일부 있는데 교육망에서는 업무시스템(나이스, K-에듀파인 등)으로의 접근을 차단하고 외부 인터넷을 통해 접근할 때와 동일하게 보안정책을 적용하여야 한다.

셋째, 교육망에서 사용하는 PC의 경우 백신을 설치하고 OS 및 백신이 최신 업데이트가 적용될 수 있도록 관리하여야 한다. 다만 별도의 백신 및 패치 관리 서버를 통해서 하지 않더라도 인터넷을 통해서 최신의 백신 및 패치가 적용될 수 있도록 최초 설치 시 적용하여야 하며 주기적인 예약검사를 통해 혹시나 발생할 수 있는 악성코드 감염을 최소화하여야 한다.

보안 준수사항

- 유선망은 자동 할당(DHCP)되는 IP가 아닌 수동으로 관리 필요
- 무선망은 유선망과 별도의 IP 대역으로 분리
- 무선망 사용 시 WPA2 이상(256비트 이상) 안전한 암호 알고리즘 사용
- 교육망에서 업무시스템(나이스, 에듀파인 등)으로의 접근 차단
- PC 내 백신 설치 및 OS와 백신에 대해 최신 업데이트 적용 관리
- 주기적인 백신 예약검사 정책 적용

2. 무선 공유기 계정 및 비밀번호 안내 시 주의사항

무선 공유기의 비밀번호 유출을 방지하기 위해 배포할 무선기기 전체를 대상으로 교직원이 직접 비밀번호를 입력하는 것은 시간적 소요가 상당하다. 이러한 소모를 줄이기 위해 교직원은 학생에게 무선기기를 배포하고, WiFi 계정 및 비밀번호를 공개할 수 있으나, 몇 가지 주의사항이 존재한다.

첫째, 학생에게 계정 및 비밀번호 안내 시 외부에 유출하지 않도록 교육이 필요하다.

둘째, 최신 기기(삼성 갤럭시 S10, 갤럭시탭 S6 이후 발매 제품)를 배포하는 경우 저장된 WiFi 비밀번호 추출이 가능하므로 주의해야 한다.

안드로이드 저장된 와이파이 비밀번호 확인하기

QR코드를 이용한 와이파이 프로필 공유 기능은 암호화가 되어있지 않기 때문에 QR코드 안의 데이터를 열어보면 와이파이의 SSID와 비밀번호를 확인할 수 있으며 이를 이용해 우회적으로 와이파이 비밀번호를 확인할 수 있습니다.

윈도우10 와이파이 비밀번호 찾기

무선 속성에서 보안 탭을 클릭한 다음 나오는 네트워크 보안 키의 문자 표시를 체크하면 입력되어 있는 와이파이 암호를 텍스트로 확인할 수 있습니다.

맥에서 와이파이 비밀번호 찾기

와이파이에 대한 정보가 있는 팝업이 나오면, 아래와 같이 와이파이 이름, 종류, 계정 등을 확인할 수 있습니다. 비밀번호를 확인하시기 위해서는 아래 “Show password” 옆에 있는 체크박스에 체크하시면 와이파이 비번을 확인하실 수 있습니다.

그림 7 기기별 WiFi 비밀번호 확인하기

최신 기기의 경우 기기 내부에서 WiFi 비밀번호 추출 방안을 소개하는 글을 쉽게 찾을 수 있는데, 이는 비밀번호 유출의 가능성을 높이는 지표로 볼 수 있다.

비밀번호 유출이 확인될 시, 학교에서는 해당 WiFi의 사용을 중지하고 비밀번호를 변경하여야 한다. 변경 시에는 유추하기 쉬운 비밀번호는 지양하며, 최소 8글자 이상의 숫자, 영문 대 · 소문자, 특수문자를 사용하는 등 보안 조치를 적용하여야 한다. 또한, 경우에 따라 계정정보가 외부로 유출될 가능성이 매우 높으므로 계정을 변경하고 학생들에게 안내하여야 한다.

또한 학생과 교사 간 WiFi 로그인용 계정을 별도로 생성하고 학생용의 경우 하나의 계정으로 공용 사용이 가능하나, 교사의 경우 1인 1 계정을 생성하고 주기적으로 비밀번호를 변경하는 등 보안 조치를 적용하여야 한다.
(예시: 학년 변경 시 비밀번호 일괄 초기화 등)

보안 준수사항

- 주기적인 교육을 통해 학생에게 계정 및 비밀번호 안내 시 외부에 유출되지 않도록 주의
- 무선 WiFi 접속용 비밀번호는 유추하기 쉬운 비밀번호 사용 지양 및 최소 8자리 이상의 숫자, 영문 대 · 소문자, 특수문자를 혼합하여 설정
- 주기적인 계정정보 변경
- WiFi 접속용 계정은 교사와 학생 간 분리하고 교사는 1인 1 계정 사용
- 주기적인 비밀번호 변경

3. 최신 보안 업데이트 적용

일반적으로 사용자들은 보안패치의 업데이트 메시지를 자주 발견할 수 있다. 보안패치는 프로그램과 소프트웨어의 보안상 취약점을 보완하여, 악성코드의 감염 및 각종 오류의 원인을 제거하는 역할을 한다.

그러나, 사용자의 보안 의식 부족으로 인해 보안 업데이트를 최신으로 유지하지 않는 경우, 쌓여있는 업데이트의 버전 만큼이나 취약점을 내포하게 된다.

그림 8 보안문제로 인한 OS 업데이트 사례

따라서 학생에게 배포한 기기는 반드시 기기(OS) 업데이트를 진행하고, 사용 앱은 최신 버전 사용을 권장하며, 주기적으로 관리하여야 한다.

❶ 안드로이드 기기

그림 9 안드로이드 OS 기기 자동 업데이트 설정

실행순서 : ❶ 설정 → ❷ 소프트웨어 업데이트 → ❸ WiFi로 자동 다운로드

❷ iOS 기기

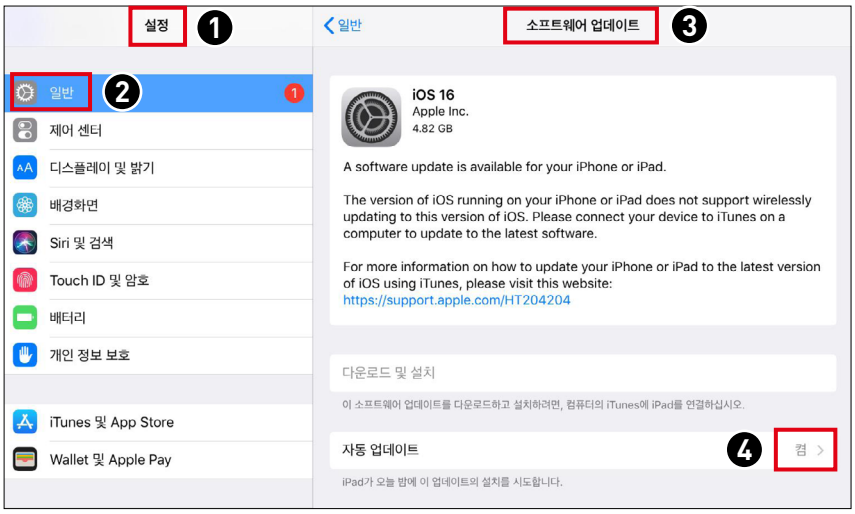

그림 10 iOS 기기 자동 업데이트 설정

실행순서 : ❶ 설정 → ❷ 일반 → ❸ 소프트웨어 업데이트 → ❹ 자동 업데이트 켬

다만 학교에서 사용하는 무선기기는 학교별로 기기의 수량, 관리 인원의 유무 등 다양한 요소가 존재하므로 관할 시도교육청에서 학교에서 사용하는 모바일 기기에 대한 통합유지보수를 통해 최신 업데이트를 적용하는 방법을 권고하며 각각의 현장에 적절한 방법을 선택하여 실행하여야 할 것이다.

4. 개인기기 사용 시 유의점

모바일 및 노트북의 수요가 증가함에 따라 학생들은 초 · 중등학교에서 배포한 기기 외에도 개인기기를 소지할 가능성이 있다. 학생이 개인기기를 사용하여 학교의 무선 공유기에 접속하고자 할 때, 아래의 몇 가지 주의 사항을 사전 안내할 필요성이 있다.

첫째, 학생이 사용하고자 하는 개인기기의 보안 업데이트 버전이 최신이어야 한다. 업데이트 버전이 최신이 아닐 경우, 해당 기기가 포함한 취약점을 통해 무선 공유기가 공격 목표가 될 수 있으므로 접속이 차단되거나 제약을 받을 수 있다.

❶ 안드로이드 기기

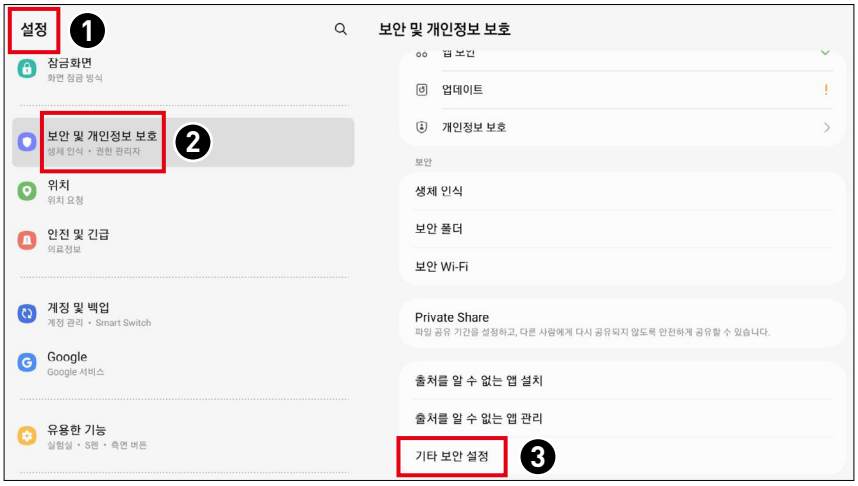

그림 11 안드로이드 기기 보안 업데이트 설정 ①

실행순서 : ❶ 설정 → ❷ 보안 및 개인정보 보호 → ❸ 기타 보안 설정

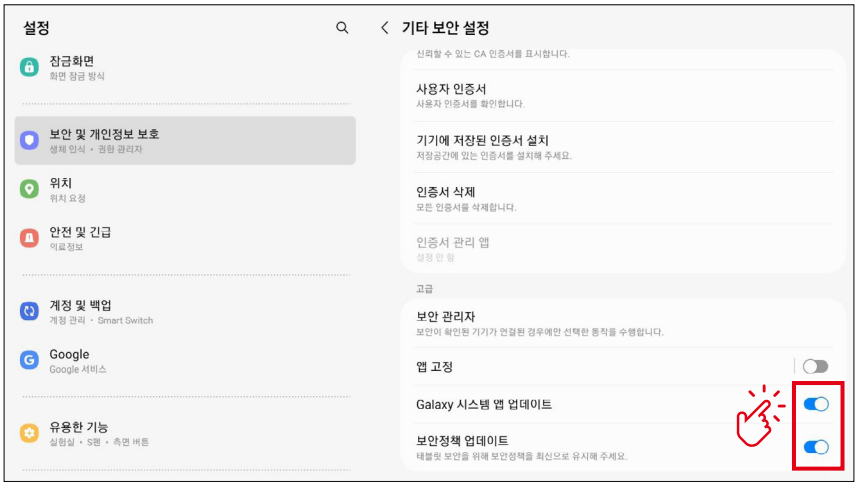

그림 12 안드로이드 기기 보안 업데이트 설정 ②

❷ iOS 기기

그림 13 iOS 기기 보안 업데이트 설정

(그림 10 의 ④ 다음 화면의 마지막 항목 켜기)

둘째, 앱 스토어 구매 등 정상 경로를 통해 설치된 앱이 아닌 경우 접속이 차단될 수 있다. 불법다운로드로 설치된 앱이 존재할 시 해당 기기를 통해 무선 AP에 접속하여 타 기기에 악성코드 등이 배포될 위험이 있으므로 기기의 보안 설정 완료 여부를 확인하여야 한다

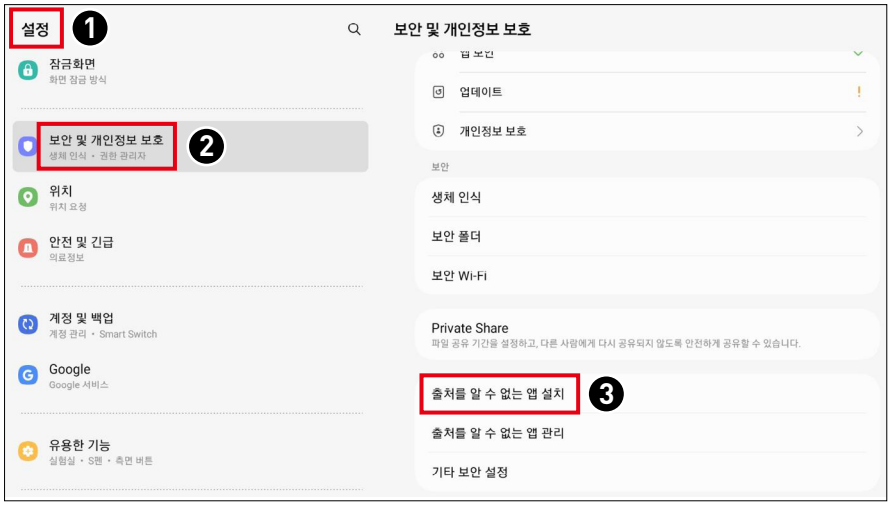

그림 14 안드로이드 기기 출처 불명 앱 차단 ①

실행순서 : ❶ 설정 → ❷ 보안 및 개인정보 보호 → ❸ 출처를 알 수 없는 앱 설치

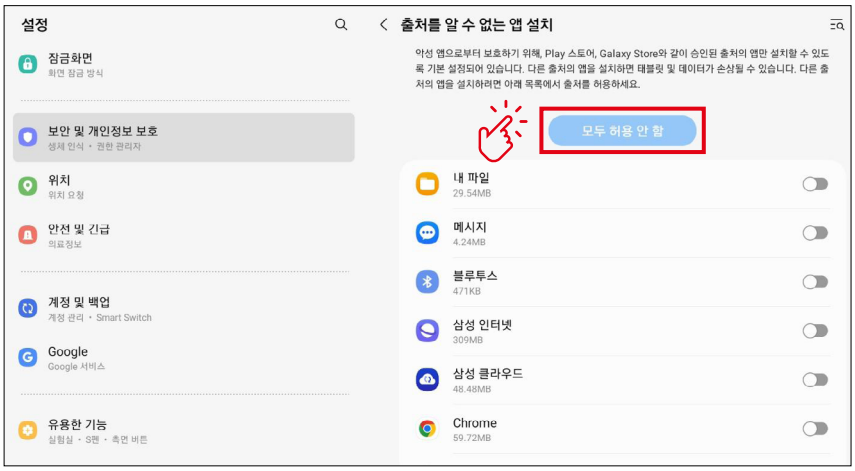

그림 15 안드로이드 기기 출처 불명 앱 차단 ②

하지만 학생이 소지한 개인기기가 최신보안이 설치되었는지, 정상적인 앱만 사용하는지 직원이 전부 파악하기에 무리가 있다. 이에 따라 주기적으로 학생에게 주의 사항을 충분히 고지하고 학교에서 배포된 기기 외의 접속 및 사용은 줄이는 것이 해킹의 위험을 낮추겠지만, 개인기기를 사용하는 경우 개인기기 자체의 보안성을 높이고 불법다운로드 및 설치는 지양하며, 피싱 메일에 주의하는 등 외부에 유출되지 않도록 사전에 조치해야 한다.

보안 준수사항

- 최신 보안 업데이트가 완료된 기기만 연결
- 정식 배포 경로(앱 스토어 등)에서 설치한 앱이 아닌 경우 접속 차단
- 주기적으로 학생에게 개인기기 보안 사항 고지

5. 유·무선망 혼용 사용 시 유의점

모바일 기기의 수요 증가에 따라 학교에서도 노트북을 학습용으로도 사용하고 동시에 유선 랜을 연결하여 업무용으로도 혼용하여 사용하는 경우가 증가하고 있다. 특히 한 대의 노트북을 통해 학습 및 업무용 PC로 동시에 사용하여 예산을 절감하고 편의성을 높일 수 있어 많은 학교에서는 기존의 PC 대신 노트북을 사용하는 경우가 늘어나고 있다.

하지만 이렇게 한 대의 노트북으로 학습과 업무에 동시 사용하는 경우 인터넷을 통해 유입된 악성코드가 노트북을 통해 업무망으로 유입되어 나이스 등 중요 업무시스템을 공격할 수 있는 경로로 악용될 수 있다.

이러한 문제를 해결하기 위해서 업무망의 경우 지정된 MAC 주소를 인증받고 백신 및 패치 관리시스템을 활용하여 최신 백신 및 보안 업데이트를 적용하고 있으나 근본적인 해결 방법이 되기는 어렵다. 왜냐하면 실질적으로 악성코드가 감염되었을 때 연결되어 있는 모든 시스템에 공격이 수행되어 감염되기 때문이다.

따라서, 한 대의 노트북(또는 PC)으로 유 · 무선을 혼용하여 사용하는 경우 주기적으로(매일) 백신 검사를 해야 한다. 네트워크를 변경하기 전에도 백신 검사를 하고 보안 설정을 적용하여 망간 혼용으로 인한 업무망 악성코드 감염이 일어나지 않도록 주의하여야 한다.

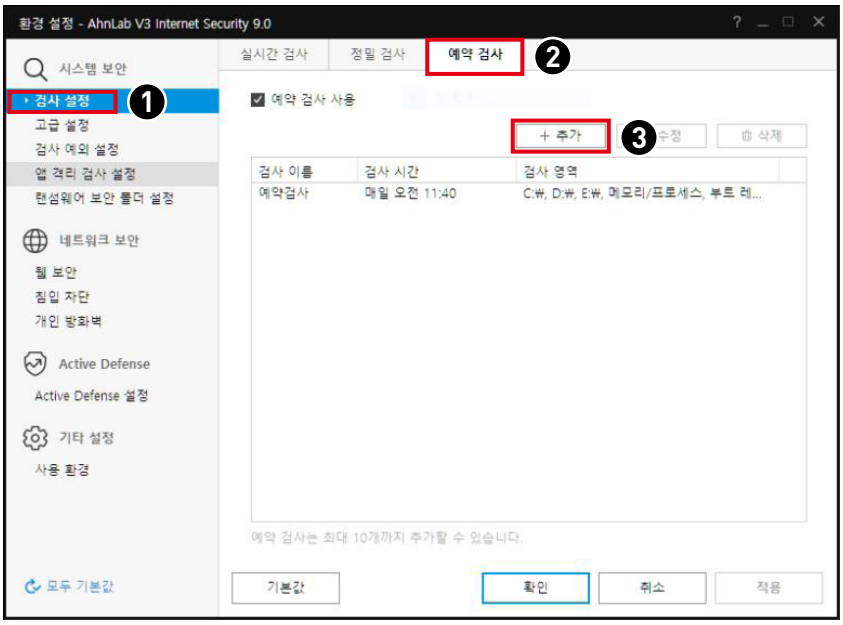

그림 16 V3 백신 자동검사 설정 ①

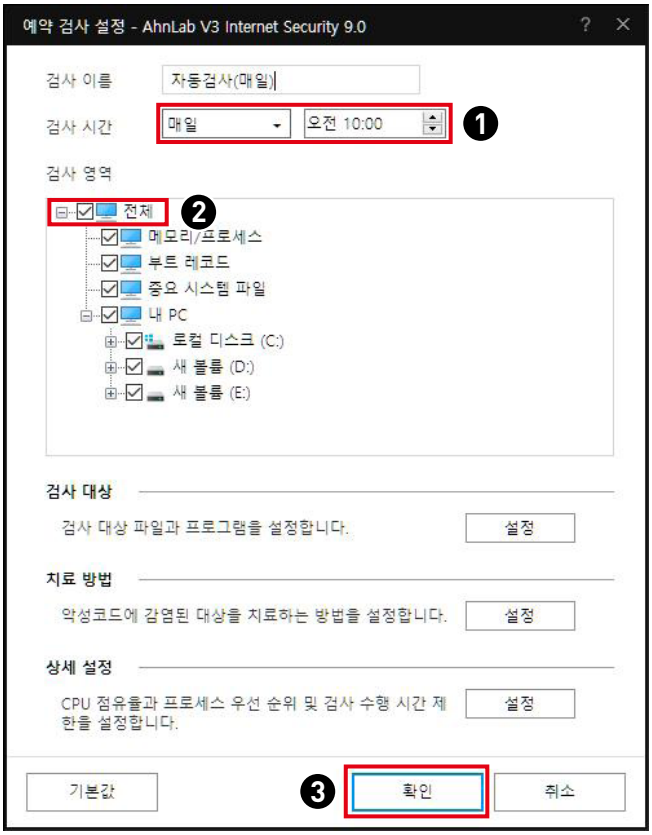

그림 17 V3 백신 자동검사 설정 ②

보안 준수사항

- 한 대의 노트북(또는 PC)으로 유 · 무선을 혼용하여 사용하는 경우 주기적으로(매일) 백신 검사
- 네트워크 변경 전 백신 검사 실시

6. 민간 클라우드서비스 사용 시 유의점

교육망의 경우 관련 지침에 따라 민간 클라우드서비스(구글 문서, 마이크로소프트 365 등) 및 화상회의시스템(Zoom, 구글 Meet 등) 사용이 가능하다. 다만 민간 클라우드서비스를 사용할 때는 자유롭게 이용은 가능하나 최소한의 보안 조치를 적용하여 민간 클라우드서비스 사용으로 인한 정보 유출 등을 방지하여야 한다.

첫째, 로그인 시 2차 인증을 적용하여야 한다.

그림 18 구글 드라이브 2차 인증 적용

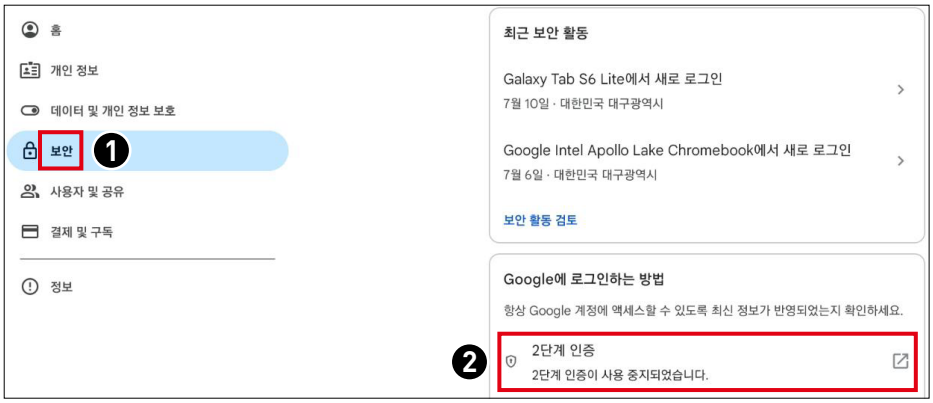

그림 19 구글 드라이브 2차 인증 적용

실행순서 : ❶ 보안 → ❷ 2단계 인증

최근 다양한 경로를 통해 개인의 비밀번호가 유출되고 다수 시스템에서 동일한 비밀번호를 사용하는 경우가 늘어나면서 클라우드 시스템이 아닌 다른 홈페이지의 비밀번호를 통해 클라우드의 정보가 유출되는 경우가 발생하고 있다. 이러한 문제를 해결하기 위해서 클라우드 로그인 시 2차 인증을 필수로 적용하여야 한다.

2차 인증에서는 OTP(One Time Password), 핸드폰 알람을 통한 인증 여부 확인 등이 있으며 해당 클라우드에서 지원하는 2차 인증 방법 중 개인의 접근이 편리한 OTP, 알람 인증 적용을 권고한다.

해외사례

"2014 Celebrity nude photo leak" 사건

역대 최대 규모의 할리우드 유명 인사들의 나체사진 유포 사건.
– 구글, 애플 서비스로 위장한 메일을 발송하여 아이디와 비밀번호, 본인 확인 정보 등을 습득
– 해당 정보를 활용 애플 iCloud*에 접속하여 사진을 다운로드 및 유포
*애플사에서 제공하는 자료 저장용 클라우드서비스
– 해당 사건 이후 iCloud 이용 시 이중 인증을 의무화

둘째, 클라우드 사용 시 자료 보안에 유의하여야 한다. 클라우드의 경우 자료의 공유가 자유롭고 손쉽게 데이터 저장이 가능하다는 장점이 있으나 무심코 저장된 자료 중 개인정보나 중요 업무자료가 포함될 수 있기 때문이다. 따라서, 지정된 폴더에 대한 자동 동기화가 아닌 수동 업로드 기능을 사용하여 업로드 시 자료의 개인정보 포함 여부 등을 사전에 점검하여 주요 자료가 클라우드를 통해 외부로 유출되지 않도록 주의하여야 한다.

그림 20 구글 드라이브 자동 백업 설정

실행순서 : ❶ 설정 → ❷ 백업 및 재설정(기기 백업 설정)

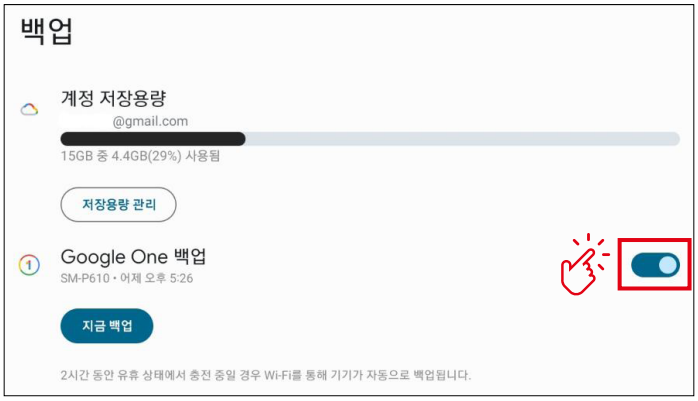

그림 21 구글 드라이브 자동 업로드 해제

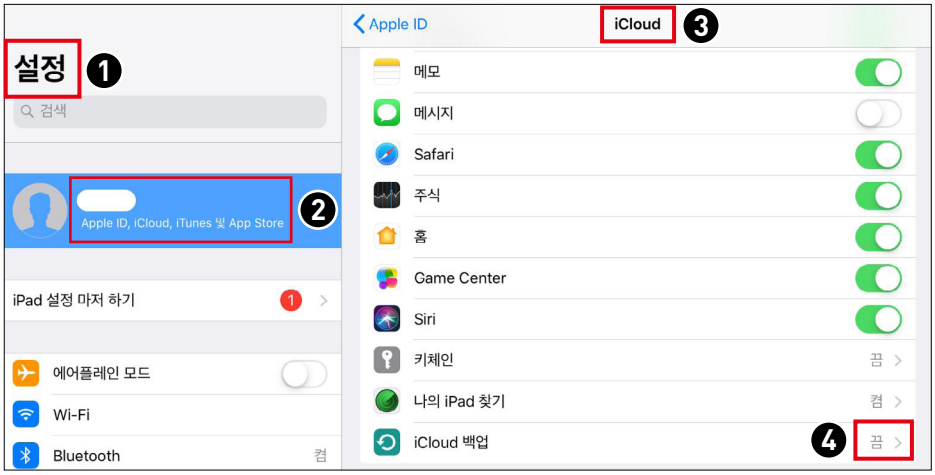

그림 22 iCloud 자동 업로드 해제

실행순서 : ❶ 설정 → ❷ Apple ID, iCloud, iTunes 및 App store → ❸ iCloud → ❹ 끔

셋째, 클라우드 또는 화상회의 앱을 사용할 때 안드로이드의 경우 구글 Play Store(갤럭시 Store 포함), 아이폰(아이패드 포함)의 경우 애플의 App Store에서 제조사 공식 버전을 사용하여야 한다. 그 외에서 다운로드 받은 앱을 사용하는 경우 위 · 변조를 통해 개인의 정보와 자료 등을 외부로 유출하거나 모바일 기기의 원격 조작을 통해 추가 정보가 유출될 가능성이 있으므로 제조사 정식 앱을 사용하도록 한다.

보안 준수사항

- 민간 클라우드 로그인 시 2차 인증 적용
- 지정된 폴더에 대한 자동 동기화가 아닌 수동 업로드 기능을 사용
- 업로드 시 자료의 개인정보 포함 여부 등을 사전에 점검
- 클라우드 또는 화상회의 앱 사용 시 공식 앱 사용

붙임 학교 인터넷 보안 준수사항 체크리스트

구분	유형	보안 준수 사항	비고
업무망	운영기준 (p8)	CMOS · 로그인 비밀번호의 정기적 변경 사용 및 PC 보안 관리 강화	
		최신 백신 및 소프트웨어 보안패치 유지	
		신뢰할 수 있는 사이트 및 프로그램 사용	
		인터넷 파일 공유(토렌트, 웹하드, P2P 등) · 메신저 등 업무상 불필요한 프로그램을 설치하지 아니하도록 하며, 이에 대한 지속적인 관리	
		웹브라우저를 통해 서명되지 않은 액티브-X가 다운로드 · 실행되지 않도록 보안 설정을 적용하여야 하며 다운로드 된 실행파일은 백신으로 점검 후 사용	
	학교 내 서버가 있는 경우 (p9)	서버 관리를 위한 별도의 PC를 마련하여야 하며 외부 인터넷을 통해 데이터를 주고받을 때는 망연계 시스템 사용	
		학교 내 별도 망연계 시스템이 없는 경우 학교장 책임하에 보안 USB 사용	
		서버 운영 시 학교 내 관리자 지정 및 주기적 관리	
		시도교육청은 학교 내 설치되어 있는 서버의 IP 관리, 보안 조치 확인 등 주기적 관리 감독	
		학교 내 서버 설치 시 서버 구성 및 저장자료 등을 확인하여 보안성 검토	
	학교 외부에 서버가 있는 경우 (p11)	학교에서는 해당 업무용 PC에 대한 관리자를 지정하고 주기적인 보안 관리 여부 점검	
		업무 담당자 외 PC 임의 사용 제한	
		업무용 PC에서 접근이 가능한 시스템을 한정하고 불필요한 서비스에 접근하는 것을 차단	
		내PC지키미 등 PC 점검 도구를 사용하여 주기적인 보안 관리	
		사업 수행 시 입력 데이터 등에 대한 보안성 검토	
	민간 클라우드 서비스 이용 시 유의점 (p12)	구글 문서, 마이크로소프트 365 등 보안인증 받지 않은 민간 클라우드서비스의 경우 교육용으로 용도를 한정하고 업무용으로 사용 금지	
		업무 목적을 위해 민간 클라우드 이용 시 보안성 검토	
		민간 클라우드서비스 사용 시 네트워크 암호화(SSL 등) 적용과 로그인 시 2차 인증 적용	
		민간 클라우드서비스 내 개인정보 포함 시 개인정보 안정성 확보조치 및 업무 위탁에 따른 보안 조치 적용	

붙임 학교 인터넷 보안 준수사항 체크리스트

구분	유 형	보안 준수 사항	비고
업무망	민간 메신저 이용 시 유의점 (p13)	비공개 업무자료의 경우 민간 메신저를 통해 유통되지 않도록 주의	
		자료를 민간 메신저를 통해 유통하는 경우 중요자료가 포함되지 않도록 사전 검토 필수	
		필요시 자료에 별도 암호를 걸어서 유통하는 등 외부 유출 방지 조치	
		메신저 로그인 비밀번호는 정기적으로 변경하고 2차 인증 적용	
		메신저에 대한 자동 로그인 기능 비활성화	
교육망	운영 기준 (p14)	유선망은 자동 할당(DHCP)되는 IP가 아닌 수동으로 관리	
		무선망은 유선망과 별도의 IP 대역으로 분리	
		교육망에서 교육정보시스템(나이스, 에듀파인 등)으로의 직접 접근 차단	
		PC 내 백신 설치 및 OS와 백신에 대해 최신 업데이트 적용 관리	
		주기적인 백신 예약검사 정책 적용	
	무선 공유기 계정 및 비밀번호 안내 시 주의사항 (p19)	주기적인 교육을 통해 학생에게 계정 및 비밀번호 안내 시 외부에 유출되지 않도록 주의	
		무선 WiFi 접속용 비밀번호는 유추하기 쉬운 비밀번호 사용 지양 및 8자리 이상의 숫자, 대 · 소문자, 특수문자를 혼합하여 설정	
		주기적인 계정정보 변경	
		WiFi 접속용 계정은 교사와 학생 간 분리하고 교사는 1인 1계정 사용	
		주기적인 비밀번호 변경	
	개인기기 사용 시 유의점 (p19)	최신 보안 업데이트가 완료된 기기만 연결	
		정식 배포 경로(앱 스토어 등)에서 설치한 앱이 아닌 경우 접속 차단	
		주기적으로 학생에게 개인기기 보안 사항 고지	
	유·무선망 혼용 사용 시 유의점 (p22)	유무선을 한 대의 노트북 또는 PC로 혼용하여 사용하는 경우 주기적(매일)으로 백신 검사	
		네트워크 변경 전 백신 검사 실시	
	민간 클라우드 서비스 사용 시 유의점 (p24)	민간 클라우드 로그인 시 2차 인증 적용	
		지정된 폴더에 대한 자동 동기화가 아닌 수동 업로드 기능을 사용	
		업로드 시 자료의 개인정보 포함 여부 등을 사전에 점검	
		클라우드 또는 화상회의 앱 사용 시 공식 앱 사용	