비대면 업무환경(원격근무, 영상회의) 도입·운영을 위한 보안 가이드

2020. 6.

과학기술정보통신부

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

목 차

1. 개 요

1) 배경

o 코로나19 확산으로 인한 '사회적 거리 두기' 시행과 직장내 확진자 발생에 따른 근무장소 폐쇄 등으로 인해 비대면 업무방식 확산

- 공무원 교대 재택근무 의무화[1] 및 비대면 근무 활성화[2] 등 공공영역에 대한 인사혁신처 근무지침 시행
- 기업의 크기·업종에 상관없이 다양한 기업들이 재택근무 시행[3][4]

o 비대면 업무 환경(원격근무, 영상회의)이 가지는 특성과 보안 위협을 정의하고 침해사고 예방을 위해 필요한 보안 강화 방안 안내

2) 주요 내용

o **(비대면 업무 환경 이해)** 비대면 업무 환경 정의 및 구성 요소 소개

- 비대면 업무 환경이 무엇인지 정의
- 비대면 업무 환경을 구성하는 요소 및 해외 주요 현황 소개

o **(주요 보안 위협 소개)** 비대면 업무 환경이 가지는 보안 위협과 사례

- 비대면 업무 환경에 대한 물리적/인적/기술적 보안위협
- 비대면 업무 환경에서 발생한 침해사고 사례

o **(보안 강화 방안 안내)** 세부 보안 지침 및 보안 점검 항목 소개

- 업무 수행 주체(원격 근무자, 시스템 관리자)에게 요구되는 보안 수칙
- 원격 근무와 영상회의 환경에 대한 보안 점검 체크리스트

---

1) 사회적 거리두기' 공무원 복무 관리 특별지침 시행, 인사혁신처, http://www.korea.kr/news/cardnewsView.do?newsId=148870748
2) 공무원 비대면 근무 활성화…인사혁신처 근무지침 시행, KBS, https://world.kbs.co.kr/service/news_view.htm?lang=k&Seq_Code=355701
3) 대기업도 '코로나19'초비상.."직원 감염 막아라" 재택근무 확산, 시사주간, https://www.sisaweekly.com/news/articleView.html?idxno=30874
4) [좋은 기업 리스트 박제] 재택근무 현황!, 잡플래닛, https://www.jobplanet.co.kr/companies/351293/story/컴퍼니%20타임스?content_id=486

2. 비대면 업무 환경 이해

가. 원격근무

1) 원격근무 정의

o 업무 수행자가 기업 및 기관 내부의 정해진 사무 공간이 아닌 외부 다른 공간에서 업무를 수행하는 것을 통칭함

- 재택근무 또는 출장으로 인해 외부에서 기업 및 기관 내부 시스템에 접속하여 업무를 처리하는 수행 방식이 원격근무에 해당됨
- 원격근무를 위해서는 외부에서 회사 내부의 업무처리 시스템으로 안전하게 접속할 수 있는 방법을 제공하는 것이 가장 중요함
- 원격근무 시 주로 접속하게 되는 기업의 업무처리 시스템은 '그룹웨어'와 '전사적 자원 관리 시스템(ERP)'이 있음
- 해외에서는 원격근무가 꾸준히 증가해왔으며, 국내의 경우 COVID-19의 영향으로 최근 급격하게 증가하고 있음

< 해외의 원격근무 현황 >

- (미국) 2018년 노동 통계청 조사에서는 약 2,624만 명이 원격(재택) 근무를 시행하고 있으며 이는 2007년에 비해 159% 증가한 수치임[5)]
- (영국) 통계청에 의하면 870만 명(전체 노동인구의 약 30%)이 원격(재택) 근무를 시행하고 있음[6)]
- (호주) Indeed.com 조사 결과 약 68%의 회사가 원격근무를 허용[7)]

5) https://www.bls.gov/news.release/atus.t06.htm
6) https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/coronavirusandhomeworkingintheuklabourmarket/2019
7) http://blog.au.indeed.com/2019/01/29/report-68-australian-employers-allow-remote-working-attitudes-divided/

2) 원격근무 환경 구성 요소

o 원격근무는 인터넷으로 회사의 업무처리시스템에 접속하기 때문에 다음과 같은 구성 요소가 존재함

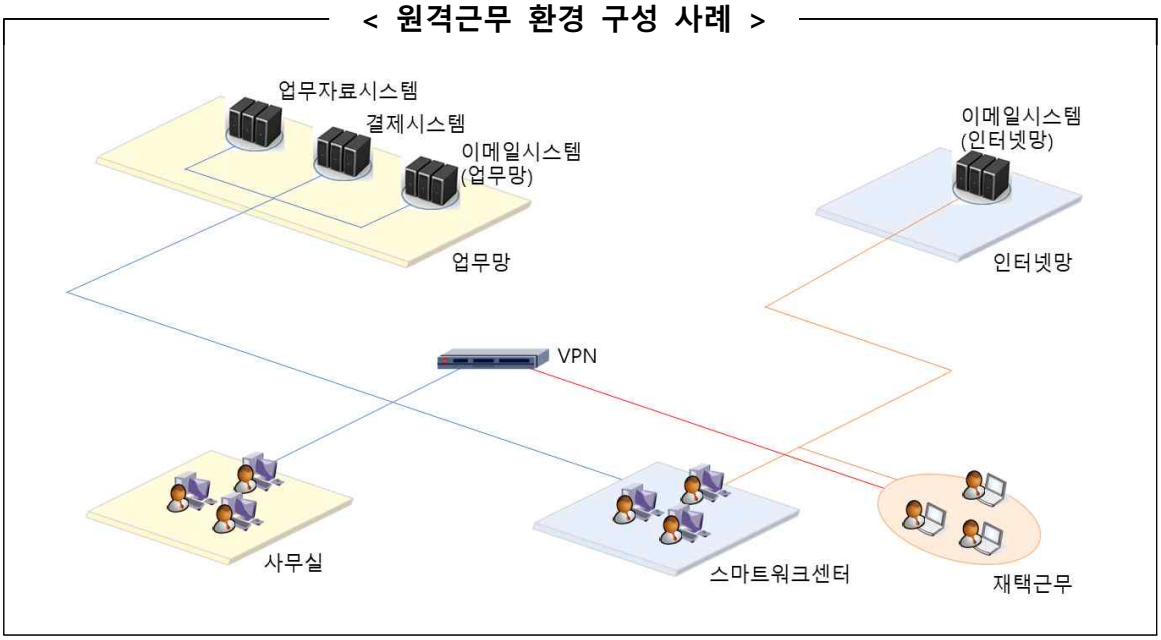
- 사용자 단말기 : PC 또는 노트북, 태블릿 또는 스마트폰

- 보안 접속 프로그램 : VPN을 사용해서 기업 업무망에 접속

※ VPN(Virtual Private Network): 단말과 회사 장비 간 암호통신을 제공함으로써 개별 사용자들이 인터넷에서도 전용회선을 사용하는 효과를 얻을 수 있음

- 업무처리 시스템 : 그룹웨어, 전사적자원관리(ERP), 이메일, 영상회의 등 기업/기관의 전산화된 업무 시스템

< 원격근무 환경 구성 사례 >



나. 영상회의

1) 영상회의 정의

o 영상회의는 물리적으로 원격에 있는 사람들이 전용장비/프로그램을 이용하여 회의를 진행하는 것을 통칭함

- 영상통화와 동일한 원리로 운영되며 다양한 기능(다자회의 기능 및 발언권 부여, 회의실 관리자 지정 등) 제공
- 이동 시간 절약 및 출장비용 감소 효과가 있으며, 신속한 의사결정을 통해 생산성을 향상시킬 수 있음
- 기업 본사와 지사(또는 해외 사무소)간의 업무 회의에 주로 사용되며, 국내에서는 원격 강의 등 교육에도 활용되고 있음
- 최근에는 직원 채용 면접이나 원격 의료에 영상회의 기술이 사용되는 사례도 있음
- 해외에서는 영상회의가 기본 업무시스템으로 인식되고 있음

< 美, 영상회의 주요 현황 >

- 매일 약 1,100만 번의 영상회의가 진행되며, 1년간 약 2.2억 번의 영상회의를 개최함. 영상회의에 사용하는 시간은 2000년 이래로 매년 10%씩 증가[8)]
- 포춘 1000 기업의 51%, 포춘 500 기업의 58%가 영상회의 서비스인 Zoom을 사용하고 있으며, 미국 Top 200 대학교의 96%가 Zoom을 사용[9)]

8) https://highfive.com/blog/10-video-conferencing-statistics
9) https://www.uctoday.com/collaboration/video-conferencing/video-success-empowering-the-channel-with-zoom/

2) 영상회의 환경 구성 요소

o 영상회의 환경에서는 원활한 의사소통을 위해 기본적으로 다음과 같은 구성 요소가 존재함

- 영상회의 플랫폼 : 회의를 위해 참여자들이 접속해서 사용하는 매개체로써 직접 구축하거나 서비스를 이용할 수 있음

< 전용 장비를 기업/기관에 직접 구축하는 방식 >

- 영상회의 시스템을 자사 전산 시스템 환경에 설치하고 운영
- 자사의 기존 업무용 시스템과 연동하는 등 맞춤형 개발 가능
- 보안 수준은 자사 전산 시스템 환경의 안전성에 종속됨
- 화상회의 시스템이 설치된 장소에서만 이용이 가능하므로 사용의 제약 발생

< 클라우드 SaaS 서비스를 이용하는 방식 >

- PC/노트북, 스마트폰 등에서 이용할 수 있는 영상회의 소프트웨어가 제공됨
- 참여자가 사용하는 단말기 환경에 따라 호환성 한계가 존재할 수 있음
- 보안 수준은 참여자가 사용하는 단말의 안전성에 종속됨
- 전용회선보다는 인터넷회선 사용을 전제로 운영하므로 통신 암호, 영상회의실 접근 통제 등의 보안 문제 발생 가능

- 사용자 단말기 : 영상회의 시스템을 사용하기 위해 이용되는 PC 또는 노트북, 태블릿 또는 스마트폰

- 화상카메라, 마이크 : 노트북, 태블릿, 스마트폰에는 기본적으로 화상 카메라가 탑재되어 있으나 PC는 별도 장착을 해야 함

- 보안 접속 프로그램 : 영상회의 시스템이 기업/기관 내부에 설치되어 있는 경우 안전한 접속을 보장하기 위한 프로그램

※ 클라우드 서비스 기반 영상회의를 사용할 경우에는 해당되지 않음

3. 비대면 업무 환경의 보안 위협

가. 원격근무 환경 보안 위협

1) 물리적 위협

o 일반적으로 원격근무 장소는 회사가 제공하는 수준의 안전한 근무 환경(단말기 유실 및 위변조 대책 등)이 보장되지 않음

o 불특정 다수가 모이는 카페, 도서관 등은 장비 도난의 위험 존재

o 이동 중 업무용 전산 장비 분실 또는 도난의 위험 존재

2) 인적 위협

o 비대면 방식으로 업무를 수행하므로 각종 사회공학적 공격에 노출될 수 있으며, 의도하지 않은 비정상 작업(행위) 발생 가능

o 회사의 중요 자료들이 원격근무에 사용되는 사용자 단말기를 통해 외부로 유출될 수 있음

o 재택근무 시 가족 및 방문자, 또는 아이들이 업무용 전산장비에 접근하여 자료를 수정하거나 삭제할 수 있음

3) 기술적 위협

o 사용자 단말기가 보안에 취약하여 악성코드에 감염될 경우 인가되지 않은 사용자(해커)의 회사 내부망 침투로 인해 피해가 확산될 수 있음

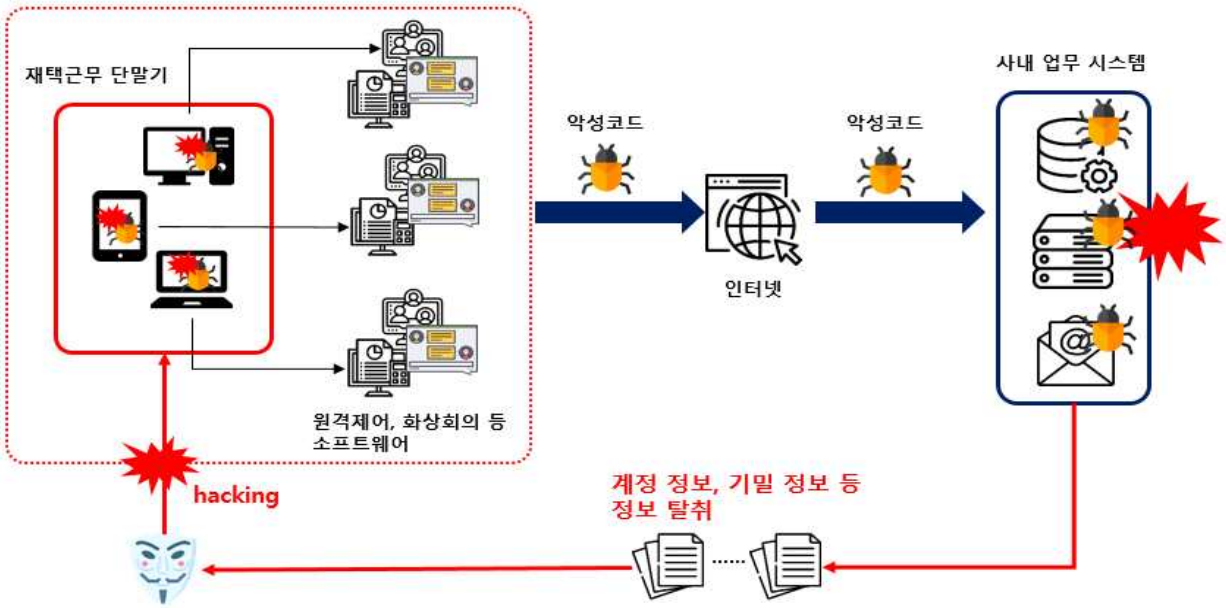
o 원격근무에 사용되는 네트워크 환경(와이파이 장비 등)이 안전하지 않을 경우 통신 내용 또는 데이터가 유출될 수 있음

o 업무 처리 시스템의 접속 인증절차가 부실한 경우, 허가받지 않은 단말기 등이 사내 네트워크에 접속할 수 있음

나. 원격근무 침해사고 사례

o 보안 기업 Avast는 자사 네트워크 침해사고 발표[10] (2019. 10. 21)

- 해커는 원격근무에 이용되는 직원의 VPN 계정 정보를 획득, 다중 인증을 사용하지 않는 보안 약점을 이용하여 기업 내부망 접근 성공
- 9월 23일에 침입을 탐지하였지만 공격은 동년 4월부터 시작한 증거를 발견함
- Avast는 공격자 행동을 관찰하려고 2주동안 의도적으로 사고 대응을 수행하지 않았으며, 공격자의 목표는 자사 도구인 CCleaner의 변조 시도였음을 확인
- 2017년에도 이와 유사한 사고가 발생한 사례가 있음[11]



<원격근무 시 발생할 수 있는 보안 위협>

다. 영상회의 환경 보안 위협

1) 물리적 위협

o 영상회의 접속 시 화상카메라와 마이크는 참가자 정보 및 회의 내용을 전달하는 통로 역할 수행

o 카메라로 보여지는 사무실 위치·개인 이력·벽에 걸린 자격증 등을 통해 사용자의 개인정보가 노출될 수 있음

10) https://www.zdnet.com/article/avast-says-hackers-breached-internal-network-through-compromised-vpn-profile/
11) https://www.zdnet.com/article/hackers-hid-malware-in-ccleaner-pc-tool-for-nearly-a-month/

o 마이크는 주변 음성을 전달하므로 의도하지 않은 추가 기밀 정보들이 마이크를 통해 타인에게 전달될 수 있음

2) 인적 위협

o 영상회의 개설자의 미비한 보안 환경설정으로 인해 허가받지 않은 사용자가 회의실에 무단으로 접속할 수 있음

3) 기술적 위협

o 영상회의 통신이 E2E(End to End) 암호화되어 있지 않은 경우 영상 및 음성내용이 노출될 가능성이 있음

o 영상회의 프로그램 또는 서비스에 취약점이 존재할 경우 추가 공격(화면 탈취, 무단 참가 등)에 악용될 수 있음

o 영상회의실 주소가 인터넷에 공개될 경우, 해당 서버를 대상으로한 디도스 공격 등으로 인해 업무 장애가 발생할 수 있음

라. 영상회의 침해사고 사례

o 2020년 3월 국내 대학 온라인 강의에서 수강생이 아닌 사람들이 강의실에 입장하여 수업을 방해하는 행위가 발생[12)]

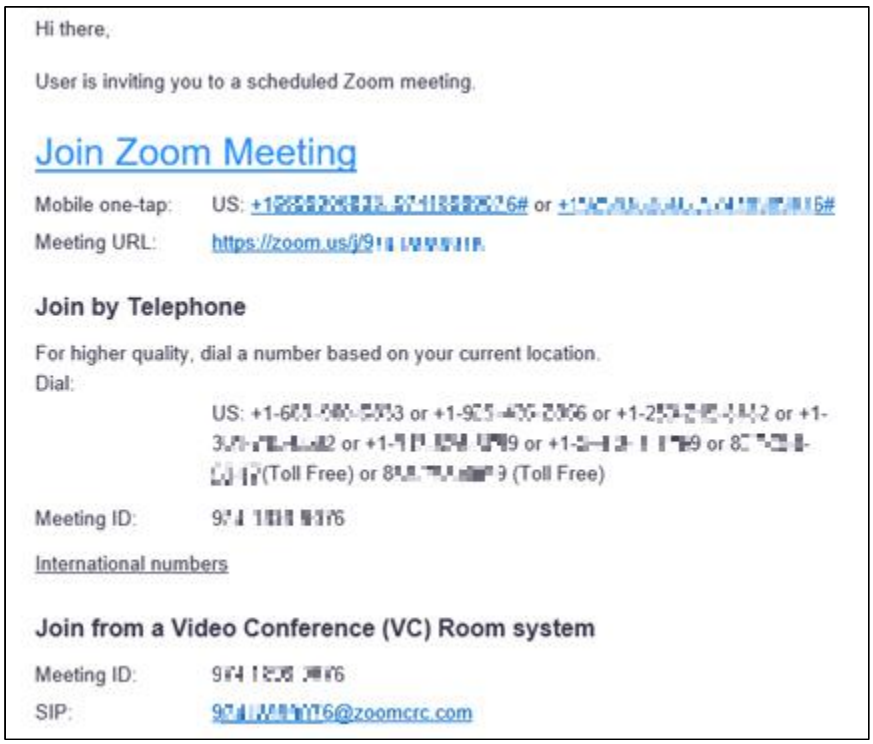
o 줌 폭격(Zoom Bombing) : 비인가 사용자가 영상회의실에 침입하여 회의를 방해하는 행위이며, 미국 FBI는 다음 사례를 공유(2020. 3)

- Zoom을 이용한 원격 강의에 허가받지 않은 사용자가 입장하여 교사를 비난하고 집 주소를 공개함
- 수업과 관련없는 사용자가 원격수업용 Zoom 회의실에 입장하여 혐오스러운 문신을 카메라로 공개함[13)]

12) https://news.joins.com/article/23733169
13) https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic

o 가짜 영상회의 초대장으로 사용자 계정을 탈취하는 공격 출현

- 영상회의를 초청하는 메일에는 회의실 주소, 회의실 입장 비밀번호와 같은 일정한 형식이 제공됨


Hi there,

User is inviting you to a scheduled Zoom meeting.

Join Zoom Meeting

Mobile one-tap: US: +1[redacted] or +1[redacted]#

Meeting URL: https://zoom.us/j/9[redacted]

Join by Telephone

For higher quality, dial a number based on your current location.

Dial:

US: +1-6[redacted]3 or +1-9[redacted]6 or +1-2[redacted]2 or +1-3[redacted]2 or +1-[redacted]9 or +1-[redacted]9 or 8[redacted] (Toll Free) or 8[redacted]9 (Toll Free)

Meeting ID: 9[redacted]6

International numbers

Join from a Video Conference (VC) Room system

Meeting ID: 9[redacted]6

SIP: 9[redacted]6@zoomcrc.com

<영상회의 초대장 메일 예시>

- 공격자는 가짜 URL이 포함된 초대장을 이용하여 사용자 로그인을 유도(계정 및 비밀번호 탈취)하거나 사용자 PC에 악성코드를 설치할 수 있음[14)]

o 영국 국방부와 미국 전기자동차 업체 테슬라는 보안 문제로 서비스형 영상회의 Zoom 사용을 금지함

- 서비스형 영상회의 대표기업인 Zoom이 E2E를 지원하지 않는 것으로 확인됨
- Zoom은 사용자 ↔ Zoom 서버 ↔ 사용자의 형태로 영상회의를 진행하며, 사용자와 Zoom 서버 구간만 암호화가 진행
- 즉, Zoom 서버에서는 암호화되지 않은 영상회의 내용이 존재하므로 데이터 유출 위험 존재
- Zoom은 문제 해결을 위해 사용자↔사용자간의 암호 방식인 E2E 지원 발표[15)]

14) https://mashable.com/article/zoom-phishing-email-hack-coronavirus-unemployment/
15) https://blog.zoom.us/wordpress/2020/04/01/facts-around-zoom-encryption-for-meetings-webinars/

4. 비대면 업무환경 보안 강화 방안

가. 원격근무 환경 도입·운영을 위한 보안

1) 원격 근무자 보안 수칙

o **(전용 공간 확보)** 카페 및 공원과 같은 개방된 장소가 아닌 보안성이 확보된 전용 공간에서 원격근무 실시

o **(단말기 보안)** 회사에서 제공된 자산(단말기)만을 사용하여 사내 네트워크에 접속해야 하며, 다른 용도로는 사용하지 않기

✓ 허가받지 않은 장비는 원격근무에 사용하지 않기
✓ 노트북, 스마트폰, 태블릿 등의 보안 업데이트를 최신 상태로 유지
✓ 원격근무 단말기에 대한 타인의 접근 제한하기

o **(프로그램 보안)** 허가된 프로그램만을 사용하고 임의로 추가 프로그램을 설치하지 않기

✓ 메신저의 경우 공개된 외부 프로그램이 아닌 사내 전용 프로그램 사용
✓ 모든 프로그램은 보안 업데이트를 최신 상태로 유지
✓ 백신, DLP, DRM 등 단말기 및 데이터 보호 프로그램 사용하기
✓ 회사에서 승인한 정당한 라이센스가 있는 프로그램만을 사용

o **(USB 등 외부 미디어 보안)** USB 사용은 가급적 제한하고, 필요시 바이러스 감염 여부 검사 등 보안대책 적용

✓ 원격근무용 단말기와 다른 컴퓨터 간 USB를 이용한 파일 복사/공유 제한
✓ 제한적 USB 저장장치 사용시, USB 자동실행 방지 및 자동 검사 설정
✓ 원격근무용 단말기 USB 포트는 읽기 전용으로만 설정
✓ 상용 클라우드 이용 금지 등 데이터 복사 및 유출에 대한 대응책 적용

o **(네트워크 보안)** 신뢰할 수 없거나 개방형 Wi-Fi는 사용하지 않고 보안성이 확보된 인터넷망 사용

✓ 홈 네트워크 사용 시 공유기의 안전한 관리자 계정/암호 설정
✓ 홈 네트워크에 허가된 사용자만 접속할 수 있도록 보안정책 적용
✓ 무선으로 접속하는 경우 암호화 방식은 WPA2 이상을 사용[16]
✓ 회사에 접속하는 경우 반드시 회사가 제공하는 안전한 접속 방법만을 사용하여 접속

o **(비밀번호 보안)** 최소 8자 이상으로 대소문자, 숫자, 특수문자 중 2종류 이상을 조합한 강력한 암호 사용 필수

✓ 업무에 사용하는 계정은 개인이 일반적으로 사용하는 계정과 반드시 구분
✓ 단말기의 보안 수준에 상관없이 브라우저에 암호를 자동 저장하지 않기
✓ 카페, 야외와 같은 개방된 환경에서는 비밀번호가 주변에 노출될 수 있으므로 가능한 전용 공간을 확보

o **(이메일 보안)** 원격근무에서는 이메일로 의사소통을 수행하므로 이를 악용한 사회공학적 공격(피싱 등)이 증가함

✓ 메일 본문에 있는 웹 사이트 링크를 함부로 클릭하지 않기
✓ 첨부파일 클릭을 유도하는 내용이 있는 경우 함부로 실행하지 않기
✓ 원격근무자가 기업 메일서버에 접속하는 경우 반드시 VPN 또는 암호통신과 같은 안전한 채널에서 접속
✓ 포털 서비스 등에서 제공하는 상용 메일을 사용하는 경우 2단계 로그인 인증 등 추가 보안 수단을 반드시 적용

16) 알기쉬운 무선랜 보안안내서, 한국인터넷진흥원, https://www.kisa.or.kr/public/laws/laws3.jsp

2) 원격근무 환경 운영자/관리자 보안 수칙

o **(통합 인증체계 운영)** 업무용 전산환경의 모든 접속은 단일 계정으로 통합 인증을 수행

- ✓ VPN 접속, 업무용 응용 프로그램 로그인 등의 계정을 통합 관리함으로써 사용자 접속 이력 및 행위 추적성 확보
- ✓ 계정을 공유할 수 없도록 제한하고 개별 사용자마다 구분된 권한을 부여하여 사용자별 이력 및 행위 추적성 확보
- ✓ 사용자 접속 이력, 접속 출발지 및 목적지 등을 지속적으로 모니터링하여 이상징후 탐지

o **(원격 근무자 인증보안)** 원격 근무자가 사내 네트워크에 접속하는 경우 다중 인증 등 강력한 인증방안 사용

- ✓ 원격근무자 접속 인증시 계정/비밀번호 외에도 추가적으로 OTP, 휴대전화 인증 등의 다중 인증 필수 적용
- ✓ 원격 근무자는 다중 접속을 허용하지 않고 하나의 인증 접속만을 허용
- ✓ 시스템 관리자 등 중요 사용자 계정은 접속 현황 집중 모니터링 적용

o **(원격접속 보안)** 허가된 사용자와 단말기만이 업무망에 접근할 수 있도록 전용 접속 환경 구축(VPN 이용 등)

- ✓ VPN 접속, 서비스 접근은 기업에서 지정한 단말기만 허용하도록 설정
- ✓ VPN으로 접속하는 단말기의 보안상태(백신 설치, 최신 보안 업데이트 적용 여부)를 점검할 수 있어야 함
- ✓ VPN으로 접속하는 사용자는 반드시 계정/비밀번호 외에 추가로 다중 인증 적용하기
- ✓ VPN 접속 시 사내 네트워크를 통해서 외부 인터넷으로 접속하도록 트래픽 경로 단일화하여 모니터링 가시성 확보

o **(원격접속 자원관리)** 원격근무자의 접속 경로인 VPN 운영 안정성 확보

- ✓ VPN IP대역 대상 디도스 공격 발생으로 원격접속 경로 자체가 차단될 수 있으므로 가용성 확보방안 마련 필요
- ✓ 디도스 공격 유형에 따른 차단정책 수립 및 적용
- ✓ 클라우드 기반 VPN을 기업 비상 접속용으로 사용 고려

o **(기업 내부망 모니터링 강화)** 사내 업무용 시스템 로그를 상시 모니터링하여 이상징후를 탐지하는 등 보안활동 강화

- ✓ VPN을 통해 접속된 원격 근무자는 기업 내부망에서 가지는 권한과 동일한 권한을 가지므로 내부망 전체의 보안 모니터링 필수
- ✓ 원격근무용 네트워크는 주소 대역을 달리하여 모니터링 용이성 확보
- ✓ 내부 업무용 서버의 보안성 강화(백신 설치, 최신 보안 업데이트, 내부 자원 모니터링) 적용
- ✓ 서버 간 불필요한 접근을 최소화하고, 필요시 계정별 권한을 부여하여 활동범위(작업범위)를 제한하는 등 접근통제 강화
- ✓ VPN 접속 현황 및 사용자 행위 이력 모니터링 등 이상징후 탐지 방안 확보

o **(비상 대응 절차 운영)** 원격 근무용 단말기의 분실 및 도난, 또는 시스템 이상징후 탐지 시 즉시 대응하는 보안 절차 운영

- ✓ 단말기 분실, 도난 등을 대비하여 원격근무 사용 단말기의 저장장치는 암호기법을 적용해서 보호
- ✓ 원격 근무 사용 계정을 중앙에서 잠금/해제할 수 있는 통제방안을 수립하고, 분실/도난 계정을 이용한 침투시도를 지속적으로 모니터링
- ✓ 필요시 원격에서 단말기의 데이터를 삭제하거나 강제 잠금을 시키는 단말기 보호기능 운영

나. 영상회의 환경 도입·운영을 위한 보안

< 플랫폼 형태별 보안성 확보방안 >

o 영상회의 플랫폼은 구축형과 서비스형이 있으며, 두 방식에 따라 보안성 확보 방안에 차이가 있음

- **(구축형)** 영상회의 전용 장비를 기업 업무망에 설치하고 직원들만 사용하는 방식

  · 영상회의 전용장비가 기업 내부 네트워크에 위치하므로 참가자는 기업에서 제공하는 인터넷망을 이용해서 접속

  · 원격근무 사용자를 위한 영상회의 S/W가 제공될 수 있으므로 단말 보안이 매우 중요

> ※ 구축형은 장비가 폐쇄망인 기업 네트워크에서 운영되므로 외부에 노출되지 않아 서비스형보다는 보안 운영이 용이하지만, 지속적인 취약점 제거를 직접 관리해야 함

- **(서비스형)** 클라우드 환경에서 제공되는 영상회의 서비스에 가입하여 사용하는 방식

  · 회의 참가자는 인터넷을 이용해서 영상회의 서비스에 접속하며, 전용 장비보다는 전용 S/W를 이용해서 접속

> ※ 서비스형은 도입 및 운영이 용이하나, 서비스 제공 업체를 통해 제공되는 범위 내에서 보안 설정이 가능하며 제공 업체의 보안 대응이 미흡할 시 위험에 노출될 수 있는 한계 존재

1) 영상회의 개설자/참가자 보안

o **(영상회의 개설자)** 영상 회의 개설시 보안 설정 및 참석자 인증 실시

✓ 영상회의를 개설할 때 반드시 회의실에 입장하기 위한 암호를 설정하기
✓ 영상회의실은 고정주소를 사용하지 않고 개설 시점에 새로운 주소 또는 새로운 회의실 번호를 사용하기
✓ 영상회의 개설자는 초대자와 참석자의 일치 여부 확인
✓ 개설자의 노트북, 스마트폰, 태블릿 등은 최신 보안 업데이트 상태로 관리

o **(영상회의 참가자)** 영상회의 참가자는 회의 참가 장소, 회의에 접속하는 S/W 및 인터넷 환경에 대한 보안성 확보

✓ 영상회의 전용 S/W에 자동 로그인 사용하지 않기
✓ 영상회의 전용 장비 및 접속 S/W의 보안 취약성을 주기적으로 검사하고 제거하기
✓ 영상회의는 반드시 암호화 통신을 설정하고 진행
✓ 영상회의 참여 인원은 회의 관련 내용이 외부로 노출되지 않도록 가급적 업무 전용 공간을 확보하여 참석하기
✓ 전용 공간을 확보하기 어려운 경우 반드시 이어폰을 사용하여 통화내역이 외부에 들리지 않게 회의 참석

2) 영상회의 플랫폼 관리자 보안

o **(구축형)** 허가된 사용자만 회사 내부의 영상회의 시스템에 접속할 수 있도록 전용 접속 환경 구축(VPN 이용 등)

- ✓ 원격 접속 및 접속 후 내부 서비스 접근은 기업에서 지정한 단말기만 허용되도록 보안 설정하기
- ✓ 원격에서 접속하는 단말기의 보안상태(백신 설치, 최신 보안 업데이트 적용 여부)를 점검할 수 있어야 함
- ✓ 원격에서 접속하는 사용자는 반드시 계정/비밀번호 이외 추가 인증 수단 적용
- ✓ 제조사에서 제공하는 영상회의 전용장비 취약점 관리를 지속적으로 수행
- ✓ VPN 접속, 업무용 응용 프로그램 로그인 등의 계정을 통합 관리함으로써 사용자 접속 이력 및 행위 추적성 확보
- ✓ 사용자 접속 이력, 접속 출발지 등을 지속적으로 모니터링하여 사용자 이상징후 탐지

o **(서비스형)** 클라우드 기반 서비스를 사용할 경우 사내 관리자가 직접 보안 설정에는 참여하지 않음

- ✓ 무료사용자와 차별성 있는 기업 전용 프로그램을 사용
- ✓ 서비스 제공 업체에서 제공하는 사용자별 데이터 암호화 등 데이터 보호 서비스 적극 활용
- ✓ 서비스 제공업체에서 제공하는 영상회의 전용 프로그램의 보안 취약점 패치를 지속 적용
- ✓ 영상회의 서비스 회사의 보안 공지는 개설자/사용자에게 신속히 공지하기
- ✓ 서비스형 영상회의 보안 설정을 개설자/사용자에게 문서 형식으로 안내
- ✓ 영상회의 서비스와 단말기 구간은 E2E(End-to-End) 암호화 통신 사용

붙임1 원격근무 환경 보안 점검 체크리스트

담당	구분	점검 내용	점검 결과
원격 근무자	근무장소	업무 수행 장소가 공개된 공간이 아닌 전용 근무 장소인가?	
	단말기 보안 관리	기업에서 지급한 원격근무용 단말기만 사내 네트워크 접속이 가능한가?	
		원격근무용 단말기(노트북, 스마트폰, 태블릿 등)는 최신 보안 업데이트 상태로 관리하는가?	
		가족, 손님 등 타인의 원격근무 단말기 사용이 불가능한 상태인가?	
	단말기설치 프로그램	원격근무용 단말기에 원격근무자가 임의로 신규 프로그램을 설치하는 것이 불가능한 상태인가?	
		원격근무자가 직원 간 대화에 사내 메신저만을 사용하고 있는가?	
		사용 모든 프로그램은 최신 보안 업데이트를 주기적으로 적용하는가?	
		백신, DLP/DRM 등 데이터 보호 프로그램을 사용하는가?	
		회사에서 승인한 정당한 라이센스가 있는 프로그램만을 사용하고 있는가?	
	USB 외부미디어	데이터 복사/전송을 위한 USB 외부 저장장치 사용을 제한하고 있는가?	
		제한적 USB 외부 저장장치 사용시, USB 자동 실행 방지 및 자동 바이러스 검사를 시행하고 있는가?	
		원격근무용 단말기의 USB 포트는 읽기 전용으로만 사용하고 있는가?	
		구글 드라이브, iCloud 등 상용 클라우드에 업무 자료 저장을 금지하고 있는가?	
	네트워크	원격근무 시 개방형 Wi-Fi를 사용한 사내망에 접속을 제한하고 있는가?	
		홈 네트워크 사용 시 공유기의 관리자 계정/암호를 안전하게 설정했는가?	
		홈 네트워크에 허가된 사용자만 접속할 수 있게 보안정책을 적용하는가?	
		무선 접속시 암호화방식은 WPA2 이상을 사용하고 있는가?	
		회사가 제공하는 안전한 접속 방법만을 사용하여 접속하고 있는가?	
	비밀번호 보안	비밀번호는 8자 이상으로 대소문자, 숫자, 특수문자 중 2가지 이상 조합하여 사용하고 있는가?	
		업무용 계정을 개인용 계정과 구분하여 사용하고 있는가?	

		사용하는 서비스 계정마다 별도의 암호를 사용하고 있는가?	
		브라우저의 암호 자동 저장하기 기능을 사용하지 않도록 하였는가?	
	이메일 보안	메일 본문에 있는 URL의 보안을 자동으로 검사하는 보안 시스템이 있는가?	
		원격근무자는 VPN을 이용해서 기업 메일서버에 접속하는가?	
		원격근무자가 메일 서버에서 클라이언트로 메일을 다운받는 경우 암호통신을 지원하는가?	
		상용 메일 사용시, 로그인 과정에 2단계 인증을 사용하고 있는가?	
		메일 시스템을 내부망과 외부망으로 구분하여 사용하고 있는가?	
기 업	네트워크 보안	지정한 단말기만 기업 네트워크에 접속할 수 있는가?	
		VPN 접속 시 원격 단말기의 보안상태(백신 설치, 최신 보안 업데이트 적용 여부)를 점검하고 있는가?	
		VPN 인증 시 다중 인증(MFA, multi-factor authentication)을 적용하고 있는가?	
		VPN 운영 및 연결자원 현황을 지속적으로 모니터링하고 있는가?	
		VPN을 대상으로한 디도스 공격에 대비하여 비상 접속 방법을 준비하고 있는가?	
	사용자 인증	기업 전산환경의 모든 접속은 단일 계정으로 통합 인증을 수행하고 있는가?	
		VPN 접속 통합인증으로 사용자 접속 이력 및 추적성을 확보하고 있는가?	
		민감한 서버 로그인/관리자 계정에 다중 인증(MFA, multi-factor authentication)을 적용하고 있는가?	
		사용자 이상징후 탐지를 위해 사용자 접속 이력, 접속 출발지 등을 지속적으로 모니터링하고 있는가?	
	기업망 모니터링 강화	SIEM 운영 등을 이용하여 기업 전산시스템 시스템 로그를 상시 모니터링하여 외부 위협 탐지를 시행하고 있는가?	
		원격근무 사용자 전용 네트워크 주소를 할당하고 있는가?	
		백신 설치, 최신 보안 업데이트, 내부 자원 모니터링 등을 통해 원격근무 사용자가 접속하는 업무시스템의 보안성을 강화하고 있는가?	
		불필요한 서버 간 접근을 최소화하고 필요시 계정별 권한을 부여하는 접근통제를 적용하고 있는가?	

붙임2 영상회의 환경 보안 점검 체크리스트

담당	구분	점검 내용	점검결과
영상회의 시스템 관리자	영상회의 (구축형)	정기적으로 영상회의 시스템의 보안 취약성을 점검하고 있는가?	
		영상회의에 접속하는 원격근무자 단말기의 보안을 점검하고 있는가?	
		기업에서 지정한 자산만이 사내 네트워크와 영상회의 시스템에 접속이 가능한가?	
		원격근무 단말기인 노트북, 스마트폰, 태블릿 등은 최신 보안 업데이트 상태로 관리하고 있는가?	
	영상회의 (서비스형)	영상회의 전용 S/W에 자동 로그인을 금지하고 있는가?	
		영상회의 서비스와 단말기 구간은 E2E(End-to-End) 암호화 통신을 지원하는가?	
		영상회의 전용 프로그램의 보안 취약점을 정기적으로 점검하고 있는가?	
		무료사용자와 일반사용자간 차별성있는 기업 전용 프로그램을 사용하고 있는가?	
		서비스 제공업체에서 제공하는 사용자 개별 데이터 암호화 등 데이터 보호 서비스 활용하고 있는가?	
	네트워크 보안	VPN등 허가된 사용자만 기업 내부망에 접근할 수 있는 전용 접속 환경을 제공하는가?	
		원격 접속 및 접속 후 내부 서비스 접근은 기업에서 지정한 단말기만 허용하도록 통제하는가?	
		원격에서 접속하는 단말기의 보안상태(백신 설치, 최신 보안 업데이트 적용 여부)를 점검하는가?	
		영상회의 접속 사용자는 계정/비밀번호 외에 추가로 다중 인증(MFA, multi-factor authentication)을 적용하는가?	
영상회의 개설자		영상회의 개설시 회의실 암호를 설정하고 있는가?	
		개설시마다 고정주소를 사용하지 않고 새로운 주소/회의실 번호를 사용하고 있는가?	
		회의 개설자는 초대자와 참석자의 일치성 여부를 검사하는가?	
		개설자가 참석자를 통제하는 기능을 사용하고 있는가?	
영상회의 참가자		영상회의에 참여하는 단말기의 및 접속 S/W의 보안 취약성을 정기적으로 검사하고 있는가?	
		암호통신 상태에서 영상회의에 참여하는가?	
		영상회의 참석 시 회의 내용이 외부로 노출되지 않는 안전한 공간에서 참석하는가?	
		전용 공간을 확보하기 어려운 경우, 이어폰을 사용하여 통화내역이 외부에 들리지 않게 회의에 참여하는가?	

붙임3 원격근무 보안 교육자료 예시

o KISA가 제공하는 각종 기술 안내서는 원격근무 및 영상회의 보안 강화에 동일하게 적용 가능한 안내서임

접속 경로 : https://www.kisa.or.kr/public/laws/laws3.jsp

▣ 알기쉬운 무선랜 보안안내서

▣ 알기쉬운 공중 무선랜 보안안내서

▣ 스마트워크 활성화를 위한 정보보호 권고 해설서

▣ 모바일 오피스 정보보호 안내서

---

o 원격근무 관련 교육 자료를 확보하지 못한 중소기업의 경우 아래 컨텐츠를 직원 교육에 활용할 수 있음

▣ 원격근무 정보보호 교육 동영상[17](한글자막 제공)

17) https://www.sans.org/security-awareness-training/deployment-kit-videos