AGR－Ⅶ－2020－②－203

금융회사 재택근무 보안 안내서

2020. 12.

금 융 보 안 원

본 안내서는 전자금융거래 법령에 따른 재택근무 시 금융회사 등이 고려해야 할 보안 고려사항을 구체적으로 안내한 것으로 안내서에 대한 질의가 있으면 금융보안 레그테크 웹페이지(regtech.fsec.or.kr)의 자문 서비스를 통해 문의

目 次

Ⅰ. 개요

□ 코로나19 등의 영향으로 **국내 금융권**에서도 **재택근무 수행 필요성**이 급증

○ 특히, 사무 환경의 밀집도가 높은 **금융권 콜센터 직원 등**을 대상으로 한 **재택근무 필요성이 지속 제기**

□ 하지만, **재택근무**는 보안 통제가 소홀할 수밖에 없는 외부에서 수행되므로 정보 유출 등 **사고 발생 우려**가 존재

[재택근무에 따른 주요 보안 위협 (출처 : 美 NIST) **]**

구 분	주요 보안 위협
외부 단말기의 물리적 통제 미흡	- 재택근무에 사용되는 외부 단말기의 분실·도난이나 타인의 정보 훔쳐보기 시 단말기 內 데이터가 유·노출 - 외부 단말기를 통한 허가되지 않은 내부 네트워크 접근
안전하지 않은 네트워크 사용	- 공용 유무선 네트워크를 통해 내부망 접속 시 도청, 중간자 공격(MITM) 등으로 중요정보가 유출
악성코드 감염에 따른 네트워크 침해	- 악성코드에 감염된 외부 단말기로 내부 네트워크 연결 시 시스템 침해 가능
내부 자원의 원격접근 위협	- 내부에서만 접근 가능했던 내부 자원에 외부 단말기도 접근 가능해짐에 따라 비인가 접근 등 보안위협

□ 이에, **금융당국**은 「**전자금융감독규정 시행세칙**」을 **개정**하여 재택근무를 위한 원격접속 시 **정보보호 통제사항을 규정***

* [별첨1] 재택근무 망분리 관련 전자금융감독규정 시행세칙
[별첨2] 전자금융감독규정시행세칙 개정안 관련 Q&A 참조

➜ **금융회사가 안전하고 신속하게 재택(원격)근무 환경을 구축할 수 있도록 필요한 보안 고려사항을 구체적으로 안내**

※ 본 안내서는 「전자금융감독규정 시행세칙」 및 美 NIST의 「재택근무 보안가이드*」 등을 참조하여 작성

* 원문 명 : Guide To Enterprise Telework, Remote Access, And BYOD Security

Ⅱ. 재택근무 시 원격접속 유형

원격접속을 통해 내부망에 접속하는 방식은 아래와 같이 **'간접 접속'**과 **'직접 접속'**으로 구분 가능하며, 재택업무 특성 및 회사 내부 환경에 따라 **접속 방식 선택** 가능

1 **(간접 접속)** 외부 단말기에서 회사 내부의 **업무용 단말기** (이하 '업무용 단말기')**를 경유**하여 내부망에 접속

[간접 접속 방식 예시]

- ㅇ 가상화 데스크톱 기반(Virtual Desktop Infrastructure, 이하 VDI) 방식
- ㅇ 원격접속 프로그램 방식

2 **(직접 접속)** 외부 단말기에서 **내부망에 직접 접속**

1 간접 접속

□ 가상화 데스크톱 기반(VDI) 방식

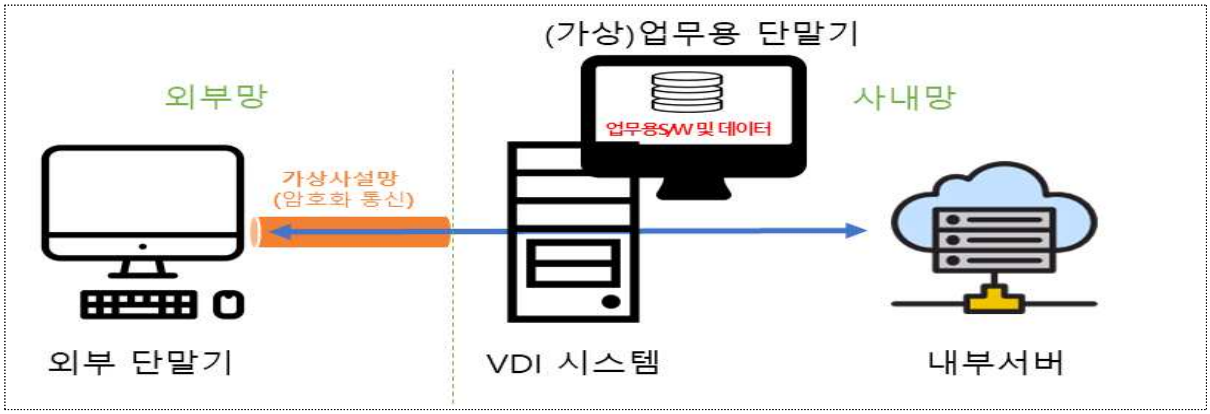
❶ **(접속 방식)** 외부 단말기에서 **VDI의 가상 업무용 단말기를 경유**하여 내부망에 접속

- ㅇ VDI는 **사내 공개망 또는 내부 업무망에 위치**할 수 있으며, 인터넷 **클라우드 기반의 VDI 서비스*** 활용도 가능

  * DaaS(Desktop as a Service) 등

❷ **(특징)** 외부 단말기가 아닌 **가상 업무용 단말기에서 업무를 처리**하며, 외부단말기에는 **가상화 데스트톱 이미지 등**만 표시

[가상화 데스크톱 기반(VDI) 방식 구조도]



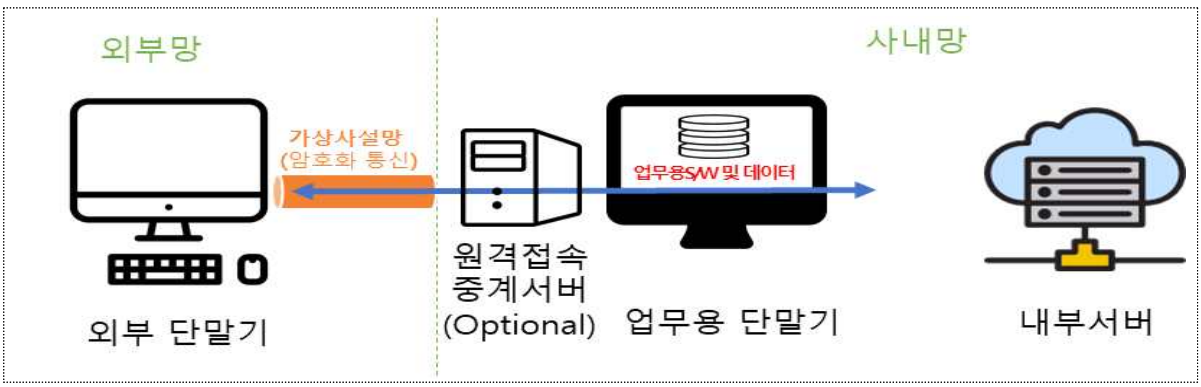
□ 원격접속 프로그램 방식

❶ **(접속 방식)** 외부 단말기에서 업무용 단말기로 **원격접속 프로그램을 이용**하여 접속

○ 외부 단말기와 업무용 단말기 간 직접 접속하거나 별도의 **원격접속 중계서버를 통한 접속**도 가능

※ 원격접속 중계서버 활용 시 중계서버에서 직원 인증, 비인가 접근제어 등 추가적인 보안기능을 지원할 수 있어 강력한 보안통제 가능

[원격접속 프로그램 방식 구조도]

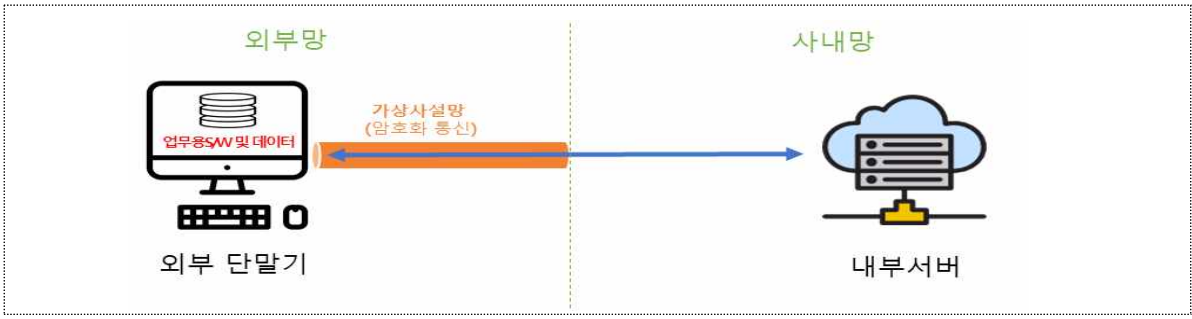


❷ **(특징)** 원격접속 프로그램 방식은 가상이 아닌 **실 업무 단말기에 접속**하여 업무를 처리

2 직접 접속

□ **(접속 방식)** 외부 단말기에서 내부의 업무용 단말기를 경유하지 않고 **내부서버 등에 직접 접속**

[직접 접속 방식 구조도]



□ **(특징)** 외부 단말기에서 업무 처리 시 **업무 데이터가 외부 단말기 내에 저장**되므로 **정보 유출 등에 대비**할 필요

Ⅲ. 원격접속 관련 보안 고려사항

1 외부 단말기 보안 관리

①공통 보안 고려사항과 ②**원격접속 유형(간접접속, 직접접속)별** '추가' 보안 고려사항으로 구분

(가) 공통 보안 고려사항

□ **(의무 사항)** 백신 프로그램 설치, **안전한 운영체제** 사용, **정보유출 방지대책 등**을 의무 적용

구 분	세부 내용
백신 프로그램 설치	- 외부 단말기에 백신 프로그램을 설치하고 실시간 탐지 정책 업데이트 및 실시간 검사 수행
안전한 운영체제 사용	- 외부 단말기는 Windows7 등 기술 지원이 종료된 운영체제를 사용하여서는 안되며, 알려진 보안패치*는 필수 적용 * 운영체제 관련 정기 보안패치 혹은 긴급 보안패치 등
로그인 비밀번호 및 화면보호기 설정	- 외부 단말기에 로그인 비밀번호 및 화면보호기를 설정하고, 일정 시간(예 : 10분) 동안 업무처리를 하지 않으면 화면 잠금 설정
정보 유출 방지대책 적용	- 외부 단말기의 화면이나 출력물 등에 의한 정보 유출 방지대책 적용 **[정보 유출 방지대책 예시]** ㅇ 화면 캡처 방지 ㅇ 개인정보 등 중요 정보에 마스킹(*) 처리 ㅇ 내부 전산자료 출력 금지 ㅇ 출력물 內 워터마크 적용 등 - 적용한 정보유출 방지대책을 직원이 외부 단말기에서 임의로 변경(삭제 또는 우회)하지 못하도록 조치

□ **(권고 사항) 개인 방화벽** 설정, **외부 단말기 도난방지** 조치, **운영체제 계정 권한** 제한 등의 적용을 권고

구 분	세부 내용
개인 방화벽 설정	- 외부로부터의 악의적인 네트워크 접근 등을 차단하기 위해 외부 단말기에 개인방화벽을 설정 ※ 이용환경(내부 또는 재택)에 따라 자동으로 보안정책을 변경하는 "자동감시(auto-sense)" 기능을 지원하는 개인방화벽의 경우, 재택근무 시 네트워크 정책 오류가 발생할 수 있으므로 재택근무 직원이 이를 자체 해결할 수 있도록 사전 교육
단말기 도난방지 조치	- 케이블 잠금장치 등을 통해 외부 단말기의 도난 등에 대비하고, 일정 시간 자리 이석 시 PC 종료 처리

○ 외부 단말기가 **모바일 기기**인 경우 **모바일 기기에 특화된 보안통제 방안**의 추가 적용을 권고

구 분	세부 내용
탈옥 된 운영체제 사용금지	- 모바일 기기 운영체제의 탈옥* 여부를 사전 검사 * 탈옥 : 모바일 기기의 모든 권한을 획득하기 위해 임의로 운영체제를 수정하는 행위를 의미
모바일 기기 잠금 설정	- 모바일 기기에 잠금을 설정하고, 잠금 설정 해제를 위한 안전한 인증 방법(바이오인증, PIN 등) 적용
불필요한 네트워크 접속 제한	- 모바일 기기에 불법적인 네트워크 접속을 차단하기 위해 NFC, 핫스팟 등의 네트워크 접속 기능은 차단
모바일 기기 통제 솔루션 적용	- 모바일 기기에 대한 강력한 통제가 필요한 경우 아래의 모바일 기기 통제 솔루션 적용 고려 ① MDM* : 모바일 기기의 보안정책 적용을 통제할 수 있는 솔루션으로, 모바일 기기(회사 지급 기기, 개인 소유 기기)별 통제 강도 조절도 가능 * Mobile Device Management ② MAM* : 모바일 기기 환경을 업무용 구간과 개인용 구간으로 분리하여 운영할 수 있는 솔루션 * Mobile Application Management

(나) 원격접속 유형별 '추가' 보안 고려사항

□ **(간접 접속 시)** 단말기 간(외부 단말기 ↔ 업무용 단말기) **파일 송수신 차단**은 의무 적용

○ 단, 간접 접속 방식 중 **원격접속 프로그램 방식**을 적용 시 보안성 확보를 위해 외부 단말기에 **추가 보안통제 적용** 필요

구 분	세부 내용	비고
파일 송수신 차단	- 외부 단말기와 업무용 단말기 간 전산자료의 송·수신이나 클립보드를 활용한 복사 전송 기능 활용 금지 - 직원이 임의로 차단설정을 변경(해제)하지 못하도록 파일 송수신 차단 조치는 외부 단말기가 아닌 회사 내부에서 설정 - 외부 단말기는 입력(키보드, 마우스 등) 및 화면 출력에 필요한 포트(port)만 접속을 허용하고 그 외의 포트는 접속을 차단하는 화이트리스트 방식 등의 적용도 고려	의무 사항
전산자료 보호	- 외부 단말기에 업무 관련 전산자료 저장 금지	권고 사항
취약한 프로그램 사용 금지	- 취약한 원격접속 프로그램을 사용을 금지 ※ 서비스 지원이 종료된 프로그램은 사용하여서는 안되며, MS社의 RDP(Remote Desktop Protocol)등 취약점이 지속 발표되고 있는 공개 소프트웨어는 미사용 권고 - 사용 중인 원격접속 프로그램에 신규 취약점 발견 시 즉시 보안패치 적용 **[원격접속 프로그램 취약점 사례]** ㅇ MS RDP 원격코드 실행 취약점(CVE-2019-0708) : Windows의 원격 터미널 접속에 사용하는 RDP에서 원격코드 실행 취약점이 발견되었으며, 공격자는 조작된 RDP 패킷을 전송하여 피해 시스템에 임의 코드 실행 가능	원격접속 프로그램 방식 적용 시 (의무 사항)
기본 포트 사용 금지	- 원격접속 프로그램의 기본 포트는 변경하여 사용	
업무용 단말기 미인가 조작 금지	- 외부 단말기가 업무용 단말기의 보안설정을 변경(백신 프로그램 실시간 탐지 중단, 개인방화벽 해제 등)하지 못하도록 조치	

업무용 단말기 전원 관리	- 업무용 단말기 전원은 원격접속 시에만 On이 되도록 하고 원격접속 종료 후에는 전원을 즉시 Off ※ 전원 On-Off의 자동화가 어려운 경우 회사에 잔류하는 필수인력 등을 통해 전원 On-Off를 조작하는 방식 등 관리적 대책 적용도 가능	원격접속 프로그램 방식 적용 시 (권고 사항)
단말기 클린(Clean) 조치	- 업무 여건상 가능한 경우(콜센터 업무 등) VDI의 가상 업무용 단말기는 업무수행 후 초기화(Clean)조치하여 업무자료의 외부 유출을 방지	VDI 방식 적용 시 (권고 사항)

○ 외부 단말기로 회사 지급이 아닌 **개인 단말기를 사용**하는 경우 보다 강력한 보안통제를 위해 **휴대 접근매체 활용 등을 권고**

구 분	세부 내용
원격접속용 휴대 접근매체 사용	- 원격접속 전용 휴대 접근매체(USB 등)를 통해 외부 단말기가 안전한 운영체제 환경에서 원격접속을 하도록 설정 - 휴대 접근매체에는 부팅(Booting) 가능한 운영체제를 탑재하고, 원격접속 전용 S/W, 보안프로그램 등 원격접속에 필요한 S/W를 사전 설치
플래시 메모리를 통한 S/W 위변조 방지	- 플래시 메모리(Flash memory)의 읽기 전용(Read-only) 영역에 재택근무용 S/W 등을 미리 설치하여 위변조 방지

□ **(직접 접속 시)** 인가되지 않은 S/W 차단 등 **외부 단말기에 추가 통제대책**을 **의무 적용**

※ 직접 접속 시 외부 단말기는 개인 단말기보다는 회사가 보안 통제를 강제할 수 있는 회사 지급 단말기를 사용

구 분	세부 내용	비고
인가되지 않은 S/W 설치 차단	- 외부 단말기의 악성코드 감염을 방지하기 위해 사내 보안정책에 따라 비 인가된 S/W는 설치를 차단	의무 사항
보안 설정 임의 변경 차단	- 재택근무자가 외부 단말기의 보안 설정을 임의 변경하지 못하도록 조치 ※ 회사에서 외부 단말기의 보안설정을 원격으로 제어하는 경우 동 제어 기능이 공격자에 악용되지 않도록 네트워크 암호화 등 보안대책 적용 필요	
외부저장장치 사용 금지	- 외부 단말기에 USB 등 외부저장장치의 읽기 또는 쓰기 기능을 차단	
전산자료 암호화 저장	- 내부 전산자료(파일, 문서)를 외부 단말기에 저장할 경우 안전한 알고리즘으로 암호화 ※ 정책적으로 전산자료는 외부 단말기에 저장하지 못하도록 통제하는 방안을 권고	
단말기 분실에 대한 보호조치	- 외부 단말기 분실 시에 대비하여 정보 유출 방지 대책(하드디스크 암호화, CMOS 비밀번호 적용 등)적용 ※ 하드디스크를 암호화하는 경우, 단말기 미사용 시 절전모드가 아닌 종료모드를 사용해야 안전하게 암호화가 가능	
이중 암호화 조치	- 외부 단말기에서 민감한 업무자료를 처리할 경우 외부 단말기 內 가상머신(VM) 환경을 구성하고 가상머신 디스크를 암호화 조치	권고 사항
자료전송 시 무결성 검증	- 업무자료를 내부 서버로 전송할 경우 자료의 무결성을 검증	

참고 **국내외에서 사용을 권고하는 대표적인 암호 알고리즘**

※ 아래 내용은 「금융부문 암호기술 활용 가이드(금융보안원)」, 「암호 알고리즘 및 키 길이 이용 안내서(KISA)」를 참조하여 재구성

구 분		대표적인 권고 알고리즘			비 고
		알고리즘		보안강도(비트)	
대칭키 암호 알고리즘		SEED		128, 256	-
		ARIA		128,192,256	
		LEA		128,192,256	
		AES		128,192,256	
해시(Hash) 알고리즘		SHA	224	112	단순 해시 및 전자서명용 해시함수 기준주) (패스워드의 안전한 저장이나 효율적인 전자서명 생성을 위한 메시지 압축 등에 사용)
			256	128	
			384	192	
			512	256	
			512/224	112	
			512/256	128	
		SHA3	224	112	
			256	128	
			384	192	
			512	256	
		LSH	224	112	
			256	128	
			384	192	
			512	256	
			512/224	112	
			512/256	128	
공개키 알고리즘	전자서명용	RSA, RSA-PSS RSASSA-PKCS#1(v1.5)		2048 이상	인수분해 기반
		DSA, KCDSA		2048 이상	이산대수 기반
		ECDSA, EC-KCDSA		224 이상	타원곡선 기반
	키교환용	RSA-KEM		2048 이상	인수분해 기반
		DH		2048 이상	이산대수 기반
		ECDH		224 이상	타원곡선 기반
	암호화용	RSA, RSAES, RSA-OAEP		2048 이상	인수분해 기반

주) 메시지 인증, 키유도, 난수생성용 해시함수는 키 길이 이용 안내서(KISA)를 참고

2 내부망 접근통제

□ **최소한의 IP 및 포트(Port)**로만 연결 허용, **미인가 IP 접속 차단** 등의 보안조치를 의무 적용

구 분	세부 내용	비 고
최소한의 IP 및 Port로만 연결 허용	- 외부 단말기가 업무상 필요한 내부 시스템에만 접속할 수 있도록 접속 가능한 IP 및 Port를 통제	의무 사항
원격접속 기록 저장	- 원격접속 사용자 정보, 접속 일시, 접속한 내부 시스템 등의 정보를 기록하고 이를 1년 이상 보관	
원격접속 시 보안조치 사전 검사	- 외부 단말기의 정보보호 필수 통제사항 적용 여부나 회사 허용 단말기 여부 등을 사전 검사 후 내부서버 등에 접속 허용 ※ 일반적으로 외부 단말기 內 NAC(Network Access Control) S/W가 설치되어 있는 경우 검사가 가능	
미인가 IP 접속 차단	- 사전에 등록(인가)된 외부 단말기만 접속할 수 있도록 미인가 IP의 접속을 제한	권고 사항

3 인증

□ 원격접속 시 **이중인증**(Multi-Factor Authentication)을 실시하고, 일정 횟수 이상 **인증 실패 시 접속차단 조치**를 의무 적용

구 분	세부 내용	비 고
이중인증 적용	- 원격접속 시 이중인증 적용 ※ 이중인증은 지식(ID/PW 등), 소유(OTP, 기기 인증 등), 특징(바이오 등) 기반 인증 수단 中 서로 다른 방식에 속하는 인증 수단을 2개 이상 조합한 인증을 의미	의무 사항

일정 횟수 이상 인증 실패 시 접속차단	- 인증 실패 횟수를 관리하고, 일정 횟수(예 : 5회) 이상 인증 실패 시 접속을 차단 - 접속차단을 해제하기 위한 별도의 본인확인 절차(접속차단 해제 신청서 제출, 유선전화 확인 등) 마련	의무 사항
서버 인증 수행	- 피싱 공격 등을 예방하기 위해 원격접속 시 직원뿐만 아니라 접속 서버에 대한 인증도 병행하여 수행	권고 사항

4 통신회선

□ 원격접속 시 통신회선은 **전용회선과 동등한 보안 수준을 갖춘 가상사설망***(VPN)을 의무적으로 구축하여 운영

* 전용회선과 동등한 보안수준을 갖춘 가상사설망은 IPSec VPN 등의 기술을 이용하여 H/W 기반으로 공용망(인터넷 등)을 전용망으로 활용하는 것을 의미

○ 단, **아래 요건을 만족**하는 **S/W기반 SSL VPN 방식 등**도 사용이 가능하며, 이 경우 **안전한 SSL 프로토콜***을 필수 적용

* SSL 3.0 이하의 프로토콜 사용 시 암호화된 데이터가 복호화되는 등의 취약점이 있으므로, TLS 프로토콜을 사용(TLS 1.3이상 권고)하여야 하며, 이를 위해 인증서버에 SSL 3.0 이하의 프로토콜 지원을 비활성화할 필요

① 전송 데이터의 기밀성 및 무결성 보장
② 클라이언트 및 서버 인증 처리
③ 중간자 공격, 재생 공격 예방

○ 누구나 접근 가능한 **개방형 SSL 접속방식**은 비인가 접근 등의 위험이 있으므로 **사용 금지**

□ VPN에는 **안전한 암호 알고리즘**을 사용하고, 내부망 접속 시 **인터넷 접속 차단 등**의 조치를 의무적으로 적용

구 분	세부 내용	비 고
네트워크 구간 암호화	- 안전한 알고리즘*으로 네트워크 구간 암호화 * 안전한 알고리즘 예시는 본 안내서 10p 참조	의무 사항
내부망 접속 시 인터넷 연결 차단	- 외부 단말기가 내부망에 접속되었으면 원격 접속에 사용되는 네트워크를 제외한 인터넷 연결을 차단 (단, 직접 접속방식인 경우 외부 단말기의 인터넷 연결을 상시 차단) **[인터넷 차단 방법 예시]** 외부와의 통신은 항시 VPN Gateway를 통하도록 하고, VPN 통신에 사용되는 LAN카드를 제외한 모든 LAN카드를 통제 * (예) VPN통신 이외의 네트워크 세션 테이블 삭제, DLP(Data Loss Protection) 솔루션 등을 통해 원격 접속에 사용된 LAN카드 이외의 모든 LAN 카드 비활성화 등	
접속 유효시간 설정	- 원격접속 후 일정 시간(예 : 15분) 업무처리가 없으면 원격접속 네트워크 연결을 차단	

5 기타

□ 재택근무자에 대한 **보안 서약서** 징구, **공공장소에서의 원격 접속 금지**를 의무 적용

구 분	세부 내용	비 고
보안서약서 징구	- 재택근무자의 보안 의식 함양 및 책임감 부여를 위해 사전 보안서약서 징구	의무 사항
공공장소 원격접속 금지	- 카페, PC방 등 공공장소에서의 원격접속 금지 - 단, 단말기의 분실·도난, 모니터 노출에 의한 정보 유출, 유무선 공유기 취약점에 의한 보안사고 위험을 통제할 수 있는 장소(예 : 공유오피스 독립 장소, 계열사 및 금융회사의 다른 건물, 내부 회의실 등)는 원격접속 가능	

Ⅳ. 재택근무 환경 구축 단계별 보안 고려사항

재택근무 환경 구축 단계를 크게 5단계*로 구분하고 단계별 보안 고려사항을 제시

* ①시작 → ②설계 → ③구현 → ④운영 및 유지보수 → ⑤폐기

(가) 시작 단계

□ 재택근무 **수행 필요성을 검토**하고, 재택근무에 필요한 **제반 사항이나 환경 등을 점검**

□ 재택근무 관련 규제*를 고려하여 **사내 재택근무 보안정책을 수립**하고 이를 **주기적으로 검토 후 필요 시 갱신**

* 전자금융감독규정 및 전자금융감독규정 시행세칙 등

○ 사내 재택근무 보안정책에는 **원격접속 유형**, 재택근무에 사용될 **외부 단말기 종류** 및 **통제 수준** 등을 포함

[사내 재택근무 보안정책 마련 시 고려사항]

구 분	주요 고려사항
원격접속 유형	- 원격접속 유형은 회사 내부 상황*을 고려하여 가장 적합한 방법은 선택하되, 회사의 보안정책을 준수 * 원격접속 대상 업무, 반영 예산, 재택근무 직원 수, IT 환경 및 성능 등
외부 단말기 종류 및 통제 수준	- 보안정책 및 기술 여건에 따라, 재택근무에 사용할 외부 단말기의 종류*를 결정 * (보유 주체) 회사 지급 단말기, 개인 단말기 (종류) PC, 모바일 기기 등 ※ 직접접속 방식인 경우 회사 지급 단말기를 이용하고, 사전에 보안 프로그램을 설치하여 제공 - 원격접속 유형에 따라 필요한 외부 단말기의 보안 통제 수준 결정 - 업무 여건상 가능한 경우 업무수행 후 외부 단말기를 초기화(Clean)하는 정책 적용도 고려

내부망 접근통제	- 업무상 원격접속이 필요한 서버를 지정 - 원격접속 기록 정보(예 : 접속자 ID, 접속 일자, 접속 시스템 등) 및 보존기간 결정 - 회사 내부 보안 정책에 따라 외부 단말기 종류(회사 지급 단말기, 개인 단말기 등)별 접근 가능한 내부 자원을 차등화 하는 방안 고려 ※ (예시) 회사 지급 단말기는 내부 통제 수준이 높아 중요 서버로의 접근도 허용할 수 있으나, 보안 통제수준이 낮은 개인 단말기는 중요도가 낮은 서버로만 제한적으로 접근하도록 허용
인증 및 통신회선	- 원격접속 시 안전한 인증 방법(이중인증) 활용 - 암호화 통신 및 인터넷 연결차단 정책 수립 - 외부 단말기의 통신회선 통제 수준을 엄격(thickness)하게 할지 유연(thin)하게 할지 결정 ※ 단, 원격접속 유형이 직접접속 방식인 경우 엄격한 통제 적용 필요 **['엄격'한 통제 수준 vs '유연'한 통제 수준 비교 예시]** ㅇ **(엄격)** 외부 단말기에서 인터넷 연결을 항시 차단하도록 통제 - 외부 단말기에서 접속 가능한 네트워크를 제한할 수 있어 강력한 보안 통제가 가능 ㅇ **(유연)** 외부 단말기에서 내부망 접속 시에만 인터넷을 차단 - 보다 자유로운 네트워크 접속이 가능한 장점이 있으나, 피싱 등 악의적인 사이트 접속 위험이 존재
기타 사항	- 재택근무자에 대한 보안서약서 징구 - 커피숍, PC방 등 공공장소에서는 단말기의 분실·도난, 모니터 노출에 의한 정보 유출, 유무선 공유기 취약점에 의한 보안사고가 발생할 수 있으므로 원격접속 금지 - 전화를 통한 업무처리 시, 유선전화의 사용을 권장하며 VoIP 서비스 등의 이용 시에는 통신 암호화 등의 대책 적용 - 근거리 무선망(WPAN)을 통한 무선 키보드, 무선 마우스, 블루투스 기기 등을 사용할 경우 공격자 악용 위험이 있으므로 주의 - 기타, 기술적으로 강제할 수 없는 통제방안의 경우, 직원 교육 등을 통해 보안 의식 함양 및 책임감 부여

(나) 설계 단계

□ 사내 재택근무 보안정책을 준수하는 원격접속 환경 구축을 위해 관련 **인프라 및 보안대책 등을 설계**하고 이를 **문서화**

[설계 단계에서의 기술적 보안 고려사항]

구 분	주요 내용
인프라 구성	- 원격접속 시스템(VDI, 원격접속 중계서버, VPN Gateway 등)의 네트워크 상 위치 및 원격접속 클라이언트 S/W를 선택 - 보안을 위해 외부 단말기 전용 네트워크 분리를 고려
인증	- 원격접속 시 인증 방법(이중인증) 선정 및 구현* 방식 결정 * (예) 인증수단 발급 및 재설정, 키배포 방법, 인증 실패허용 횟수 등
암호화	- 통신 등에 사용될 암호 알고리즘 및 암호키 길이 결정
시스템 및 단말기 보안	- 원격접속 시스템 및 외부 단말기 등에 적용할 보안대책 결정

(다) 구현 단계

□ 설계 단계에서 정한 사항을 기반으로 **원격접속 환경을 구현**하고, 실 업무에 적용하기에 앞서 **테스트 수행**

[실 업무 테스트 시 주요 점검 필요사항]

구 분	주요 내용
접근성	- 재택근무자는 필요한 내부 자원에만 원격접속을 할 수 있어야 하며, 미인가 내부 자원 접근 가능여부 확인
통신구간 보호	- 원격접속 통신구간이 안전하게 보호되어야 하며, 네트워크 모니터링 및 로그 분석 등을 통한 이상징후 검사 가능 여부 확인
인증	- 공격자가 인증을 우회할 수 없도록 무작위(robust) 테스트 수행
애플리케이션	- 원격접속 S/W가 외부 단말기, 업무용 S/W와 충돌하여 장애를 일으키지 않는지 확인

유지관리	- 관리자가 원격접속 시스템 설정을 손쉽고 안전하게 처리할 수 있는지 확인 - 외부 단말기의 보안 설정 등을 재택근무자가 임의로 바꿀 수 없는지 확인
로그기록	- 사내 재택근무 보안정책에 따라 원격접속 시 보안 로그를 기록하는지 확인
성능	- 원격접속 시스템 및 관련 장비(라우터, 방화벽 등)가 업무 피크 시에도 성능상 처리에 문제가 없는지 확인 ※ 실제 트래픽과 유사한 상황을 시뮬레이션하여 테스트할 필요
보안성	- 모든 원격접속 시스템에 최신 패치 등이 적용되었고, 필요한 경우 취약점 평가를 수행하였는지 확인

(라) 운영 및 유지보수 단계

□ 재택근무 환경 구축 후 **보안 통제의 적정성**을 정기적으로 검사

[보안 통제 적정성 검사 필요 사항]

구 분	주요 내용
보안패치 적용	- 원격접속 솔루션 및 관련 서버의 보안패치 적용 여부
시간 동기화	- 원격접속 시스템의 시간 동기화 여부
신규 보안정책 반영	- 보안정책 변경에 따른 정보보호 통제사항 반영 여부
공격 탐지	- 원격접속 환경에서 발생한 악의적인 공격 탐지 여부
관리적 보안지침 준수	- 재택근무자의 관리적 보안지침 준수 여부
로그 분석	- 주기적인 원격접속 기록 분석 여부
취약점 평가	- 원격접속 환경의 주기적인 취약점분석 평가 여부

(마) 폐기 단계

□ 외부 단말기나 업무용 단말기 등 **폐기** 시 **민감 정보는 안전한 방법으로 파기** (**모바일 기기**도 정보 삭제방안* 마련)

* (예) MDM을 통해 업무 데이터 삭제 혹은 모바일 기기 초기화 등

○ 단말기 등에 저장된 민감한 정보는 **복원이 불가**하도록 삭제하여야 하며, **사용자 접근 영역이 아닌 저장소**도 확인 후 **삭제 권고***

* (예) 윈도우 서버의 레지스트리 內 저장된 민감한 정보도 삭제 필요

Ⅳ. 시사점

□ 재택근무는 **비용 소요**가 있고 **업무 능률**이나 **보안성**에도 큰 영향을 미치므로 회사 여건에 맞는 **유연한 재택근무 환경 조성** 필요

ㅇ 콜센터 업무 등 **재택이 필요한 근무 유형**을 정하고 유형별로 **보안 통제 수준을 세분화**하여 적용

□ 재택근무 환경 구축에 있어 가장 중요한 것은 재택근무로 인해 **내부 보안 수준의 저하를 방지**하는 것임을 명심

ㅇ **재택근무 위험 요소를 최소화**하기 위해 재택근무 환경 구축부터 종료 시점까지 **철저한 보안 통제 대책 마련**이 선행

별첨1 재택근무 망분리 관련 전자금융감독규정 시행세칙 [제2조의2]

제2조의2 (망분리 적용 예외) ① 규정 제15조제1항제3호에서 금융감독원장의 확인을 받은 경우란 다음 각 호의 어느 하나와 같다

1. 내부 통신망에 연결된 단말기가 업무상 필수적으로 외부기관과 연결해야 하는 경우(다만, 이 경우 필요한 서비스번호(port)에 한하여 특정 외부기관과 연결할 수 있다).

2. 규정 제12조의 보안대책을 적용한 단말기에서 전용회선과 동등한 보안수준을 갖춘 통신망을 이용하여 외부망으로부터 내부 업무용시스템으로 원격접속 하는 경우

(중 략)

③ 제1항 및 제2항의 규정은 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 <별표7>에서 정한 망분리 대체 정보보호통제를 적용하고 정보보호위원회가 승인한 경우에 한하여 적용한다.

<별표 7> 망분리 대체 정보보호통제

<table>
<tr><th>구 분</th><th colspan="3">통제 사항</th></tr>
<tr><td>공통</td><td colspan="3">○ 외부망에서 내부망으로 전송되는 전산자료를 대상으로 악성코드 감염여부 진단·치료
○ 지능형 해킹(APT)차단 대책 수립·적용
○ 전산자료 외부전송 시 정보유출 탐지·차단·사후 모니터링</td></tr>
<tr><td>메일 시스템</td><td colspan="3">○ 본문과 첨부파일 포함하여 메일을 통한 악성코드 감염 예방 대책 수립·적용
○ 메일을 통한 정보유출 탐지·차단·사후 모니터링 대책 수립·적용</td></tr>
<tr><td>업무용 단말기</td><td colspan="3">○ 사용자의 관리자 권한 제거
○ 승인된 프로그램만 설치·실행토록 대책 수립·적용
○ 전산자료 저장 시 암호화</td></tr>
<tr><td rowspan="2">원격 접속</td><td rowspan="2">외부 단말기</td><td>공통</td><td>○ 백신 프로그램 설치, 실시간 업데이트 및 검사 수행
○ 안전한 운영체제 사용 및 최신 보안패치 적용
○ 로그인 비밀번호 및 화면 보호기 설정
○ 화면 및 출력물 등으로 인한 정보유출 방지 대책 적용</td></tr>
<tr><td>업무용 단말기를 경유하여 내부망에 접속하는 경우 (간접접속)</td><td>○ 외부 단말기와 업무용 단말기의 파일 송·수신 차단</td></tr>
</table>

		외부 단말기에서 내부망에 직접 접속하는 경우 (직접접속)	○ 인가되지 않은 S/W 설치 차단 ○ 보안 설정 임의 변경 차단 ○ USB 등 외부 저장장치 읽기/쓰기 차단 ○ 전산자료 (파일, 문서) 암호화 저장 ○ 단말기 분실 시 정보 유출 방지 대책적용(하드 디스크 암호화, CMOS비밀번호 적용 등)
	내부망 접근통제	○ 업무상 필수적인 IP, Port에 한하여 연결 허용 ○ 원격접속 기록 및 저장(예: 접속자 ID, 접속일자, 접속 시스템 등)	
	인증	○ 이중 인증 적용(예: ID/PW + OTP) ○ 일정 횟수(예 : 5회) 이상 인증 실패 시 접속 차단	
	통신 회선	○ 안전한 알고리즘으로 네트워크 구간 암호화 ○ 내부망 접속시 인터넷 연결 차단 (단, 직접 내부망으로 접속하는 원격 접속 단말기는 인터넷 연결 상시 차단) ○ 원격 접속 후 일정 유휴시간 경과 시 네트워크 연결 차단	
	기타	○ 원격접속자에 대한 보안서약서 징구 ○ 공공장소에서 원격 접속 금지	

별첨2 **전자금융감독규정시행세칙 개정안 관련 Q&A (금융감독원)**

Ⅰ. 적용 범위

1. 외주 직원들도 재택근무가 가능한지?

□ 외주 직원도 **재택근무 가능**함

○ 「전자금융감독규정시행세칙」(이하 '시행세칙') 제2조의2제1항제2호는 **모든 사내 업무용 단말기*에 대해 적용**되므로 단말기 사용자의 **소속에 따라 달리 적용되지 않음**

*「전자금융감독규정」 제15조제1항제3호의 내부통신망과 연결된 내부 업무용 시스템

2. 시스템 개발자들도 재택근무가 가능한지?

□ 전산실 내 **정보처리시스템을 직접 접속**하여 개발하는 경우 **원격접속이 허용되지 않음**

○ 시행세칙 제2조의2 제1항은 「전자금융감독규정」(이하 '규정') 제15조 제1항 제3호의 망분리 적용을 예외로 하는 것으로, 동규정 제15조 제1항 제5호의 **물리적 망분리 적용 대상자는 해당되지 않음**

3. 회사 외부에 있는 외주업체에서 전산장비 유지보수를 담당하고 있는데, 이 경우에도 원격 접속하여 유지보수가 가능한지?

□ 정보처리시스템 **유지보수 목적**의 원격접속은 **불가**

○ 시행세칙 제2조의2 제2항 제3호에 따라 전산실내 정보처리시스템에 대한 원격접속은 장애 등 **비상상황에서만 가능**

4. IT직원이 개발·보안·운영 업무가 아닌 이메일, 그룹웨어 등의 업무시스템 사용 목적의 원격접속은 가능한지?

□ IT직원도 개발·보안·운영 업무가 아닌 이메일, 그룹웨어 등의 업무시스템 사용을 목적으로 원격 접속하는 것은 가능함

5. 중요단말기도 원격접속이 가능한지?

□ 규정 제12조에 따라 중요 단말기는 외부 반출, 인터넷 접속, 그룹웨어 접속을 금지하여야 하므로 **인터넷**을 통해 **외부 기관**과 **연결**하거나, **외부 반출하여 재택근무 할 수 없음**

○ 다만, 중요 단말기는 처리 업무의 종류 및 데이터의 중요도 등 **회사 자체 기준**에 따라 지정할 수 있음

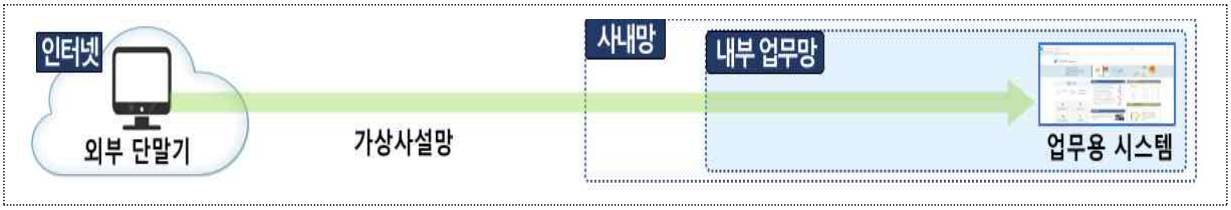
Ⅱ. 접속 방식

6. 직접 접속 방식이 무엇인지?

□ 외부 단말기가 가상사설망을 통해 **내부망의 노드(Node)로 직접 연결**

○ 외부 단말기는 **회사가** 보안 프로그램 설치, 보안 항목을 설정하여 **직접 지급**하여야 하며 **인터넷 연결을 항상 차단**하여야 함

< 직접 방식의 예시 >



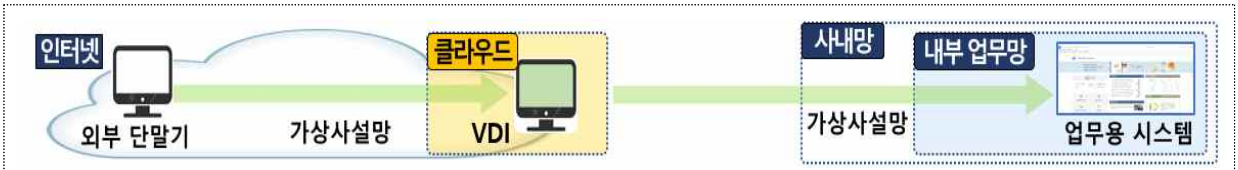
7. 간접 접속 방식이 무엇인지?

□ 외부 단말기가 **업무용 단말기를 경유**하여 내부망에 접속하는 것으로 외부 단말기는 **업무용 단말기의 입력 및 화면 출력만 처리**하고 업무용 단말기와 **파일 송수신이 차단되어야 하며, 내부망 연결시 인터넷 연결을 차단**하여야 함

< 간접 방식의 예시 >

❶ **내부망과 분리된 원격접속 전용 VDI를 경유하여 내부망에 접속**

❷ 클라우드에 있는 원격접속 전용 VDI를 경유하여 내부망에 접속



❸ 내부망에 위치한 업무용 VDI로 접속

❹ 원격접속 프로그램을 통해 내부망 업무용 단말기로 접속

☞ ❹방식은 ❶~❸ 방식보다 보안상 취약할 수 있으므로 **원격접속 프로그램에 대한 보안성 점검, 기본 접속 포트 변경, 업무용 단말기의 미인가 조작을 차단**하는 등 **보안통제를 철저히 할 필요**

8. 금융회사가 직접 접속, 간접 접속 방식으로 원격접속 방식할 수 있다고 하는데 권고하는 방식이 있는지?

□ 회사 **시스템 환경에 따라** 관련 기반기술과 방식을 **자율적으로 선택**하여 이용할 수 있음

○ 원격접속 기술 및 구현 방식 방식은 제한하지 않으나, **[별표7]의 망분리 대체 정보보호 통제**를 준수하여야 하여야 함

9. 시행세칙 제2조의2 제1항 제2호 '규정 제12조의 보안대책을 적용한 단말기'는 회사가 재택근무용으로 PC를 지급하라는 의미인지?

□ **개인PC도 이용할 수 있으나**, 원격접속 하는 외부 단말기는 규정 **제12조의 단말기 보호 대책을 만족**하여야 함

○ 다만 내부망에 자료를 전송할 수 없도록 통제장치가 되어 있는 경우(간접접속방식), 외부 단말기에 제12조의 '보조기억매체 및 휴대용 전산장비 접근통제'는 적용하지 아니할 수 있음

10. 시행세칙 제2조의2 제1항 제2호 '전용회선과 동등한 보안 수준을 갖춘 통신망'은 가상사설망(VPN) 사용이 필수인지?

□ VPN 사용을 권고하나, ①전송 데이터의 기밀성 및 무결성 보장 ②클라이언트 및 서버 인증 처리 ③중간자 공격, 재생 공격을 예방할 수 있는 다른 방식의 암호 통신도 이용 가능

Ⅲ. [별표7] 망분리 대체 정보보호 통제 관련

11. '업무용 단말기' 및 '외부 단말기'의 의미는?

□ **'업무용 단말기'**란 회사 **내부통신망*에 위치한** Desktop, Laptop, Thin Client, VDI, 태블릿 등의 단말기 (규정 제15조제1항제3호 적용 대상)

* (**내부망**) 방화벽 등으로 외부망과 구분되어 회사 외부에서는 접근할 수 없고 회사가 통제할 수 있는 범위의 사설 네트웍으로 전산센터, 본사, 백업센터, 재해복구센터, 지점 등 전용선이나 전용 사설망으로 연결된 구간

□ **'외부 단말기'**란 회사 내부통신망으로 **원격 접속 시 이용**하는 **외부망에 위치한** Desktop, Laptop, Thin Client, VDI 태블릿 등의 단말기

12. 개인 PC에도 백신 프로그램 설치 및 검사, 운영체제 버전, 로그인 비밀번호, 화면 보호기 설정 등의 보호대책을 적용해야 하는지?

□ 적용해야 함, 망분이 예외적용으로 이한 각종 보안사고를 예방하기 위해서는 **개인 단말기**에 대해 **최소한의 보안 통제 적용**은 **필요**

○ 백신 설치·업데이트 및 안전한 운영체제 이용은 일반 인터넷 뱅킹 이용자에도 적용되는 사항으로 원격접속 하는 임직원 개인PC에서도 **충분히 적용 가능**하다고 판단됨

13. 안전한 운영체제 사용 및 최신 보안패치 적용은 운영체제를 최신버전만 사용해야 한다는 의미인지?

□ 최신 운영체제를 이용하여야 한다는 의미는 아니며, **기술지원이 종료된 운영체제**는 사용하지 말아야 하고 알려진 보안 취약점에 대한 **보안 패치**는 적용되어야 함

14. 외부 단말기로 개인 PC 이용하는 경우 [별표7]의 외부단말기 공통 사항 중 '화면 및 출력물 등으로 인한 정보유출 방지대책 적용'을 위해 화면캡쳐 방지 보안프로그램 등을 적용해야 되는지?

□ '화면 및 출력물 등으로 인한 정보유출 방지대책 적용'은 화면 캡쳐 방지 보안프로그램 이외에도 **다양한 방식을 이용할 수 있음**

○ 보안프로그램 설치 외 내부 업무용 시스템 및 업무용 단말기 등에 **마스킹 처리, 워터마크** 적용 등 기타 방법으로 화면 및 출력물 등으로 인한 정보유출 방지대책 적용이 가능함

15. 평시에 회사에서 사용하는 업무용 단말기를 외부로 반출하여 재택근무시 이용할 수 있는지?

□ **가능함,** 회사에서 사용하는 업무용 단말기를 **외부로 반출**하여 재택근무용으로 **이용할 수 있으나,**

○ [별표7] '외부 단말기' 통제와 '업무용 단말기' 통제 사항을 모두 적용하여야 하며

○ 반출한 단말기는 **인터넷 연결을 항상 차단**하고 재택근무 후 **회사로 재반입 시** 내부망 연결 전 **악성코드 진단 및 치료**를 실시하여야 함

16. '원격접속 기록'은 어떤 항목을 기록하여야 하고, 얼마동안 저장하여야 하는지?

□ 원격접속 **사용자의 정보, 접속 일시, 접속한 내부 시스템** 등을 포함하고 **1년 이상 보존** (전자금융감독규정 제13조 전산자료 보호대책)

17. '이중 인증'의 인증수단으로는 어떤 것이 가능한지?

□ 인증수단을 특정하지는 않고 있으나, 지식기반·소유기반·특징기반 인증수단 중 **서로 다른 방식**에 속하는 인증수단 **2개를 조합**

18. 가상사설망은 인터넷 연결이 필수인데, '내부망 접속시 인터넷 연결 차단' 및 '인터넷 상시 차단'은 어떻게 구현할 수 있는지?

□ VPN 터널링을 위한 인터넷 연결은 가능하나 **터널링 목적 이외의 인터넷은 차단**하여야 함

○ 인터넷 차단 방법은 보안 프로그램 등을 이용하여 회사가 자율적으로 선택할 수 있음

19. 원격 접속 시 외부 단말기에서 업무상 외부망에 연결해야 하는 경우에는 어떻게 처리해야 하는지?

□ 외부단말기에서 회사 내부 업무망에 접속후 동 **내부망을 경유**하여 인터넷에 접속(**외부 단말기에서 직접 인터넷 접속 금지**)함으로써

○ 외부단말기에 회사의 기존 인터넷 보안 통제사항(유해 사이트 차단, 악성코드 방지대책 등) 등이 적용되도록 하여야 함

20. '공공장소에서 원격접속을 접속금지'는 어떤 방식으로 준수할 수 있는지?

□ 기술적으로 강제할 수 없는 통제방안의 경우, 직원교육 등을 통해 보안의식 함양 및 책임감 부여

21. 공공장소(커피숍,PC방 등)가 아닌 공유오피스 독립장소, 계열사 및 금융회사 다른 건물, 내부 회의실 등의 장소에서도 원격접속이 가능한지?

□ 가능함, 재택근무 장소를 집으로 한정하는 것은 아니나 **단말기의 분실 및 도난** 및 **모니터 노출에 의한 정보 유출, 유무선 공유기 취약점**등에 의한 **보안 사고 위험을 통제할 수 있는 장소**를 이용하여야 함

IV. 기타

22. 시행세칙이 시행된 이후에도 코로나19로 인한 재택근무관련 비조치의견서('20.2월)가 유효한지?

□ 시행세칙 개정안의 시행 시기인 **'21년 1월 1일 전까지 유효**함.

23. 현재 IT직원들은 코로나19 대응을 위해 비상대책에 따라 원격접속을 실시하고 있는데 시행세칙 시행 이후에도 코로나19가 종식되지 않을 경우 IT직원들의 원격접속은 계속 가능한지?

□ IT직원들은 장애·재해·파업·테러 등 긴급 상황 발생시 업무 연속성을 위하여 **회사 자체 비상계획**에 따라 원격접속 가능하며, 이는 이번 시행세칙 제2조의2 제1항 개정 이후에도 변동 없음

○ 다만, **'21년 1월 1일부터는 [별표7]의 개정된 사항을 반영**하여 원격접속을 실시하여야 함