IT부서 전체 자가격리 시 원격지원 (재택근무)과 보안

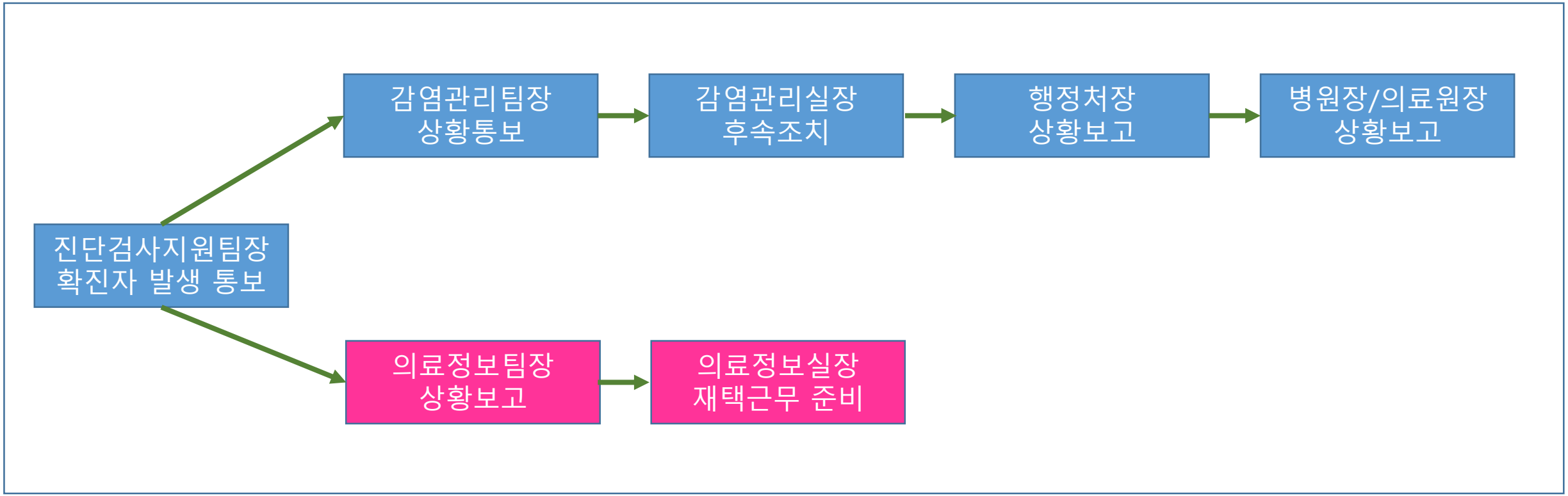
(실 사례 중심)

2020년 7월 30일

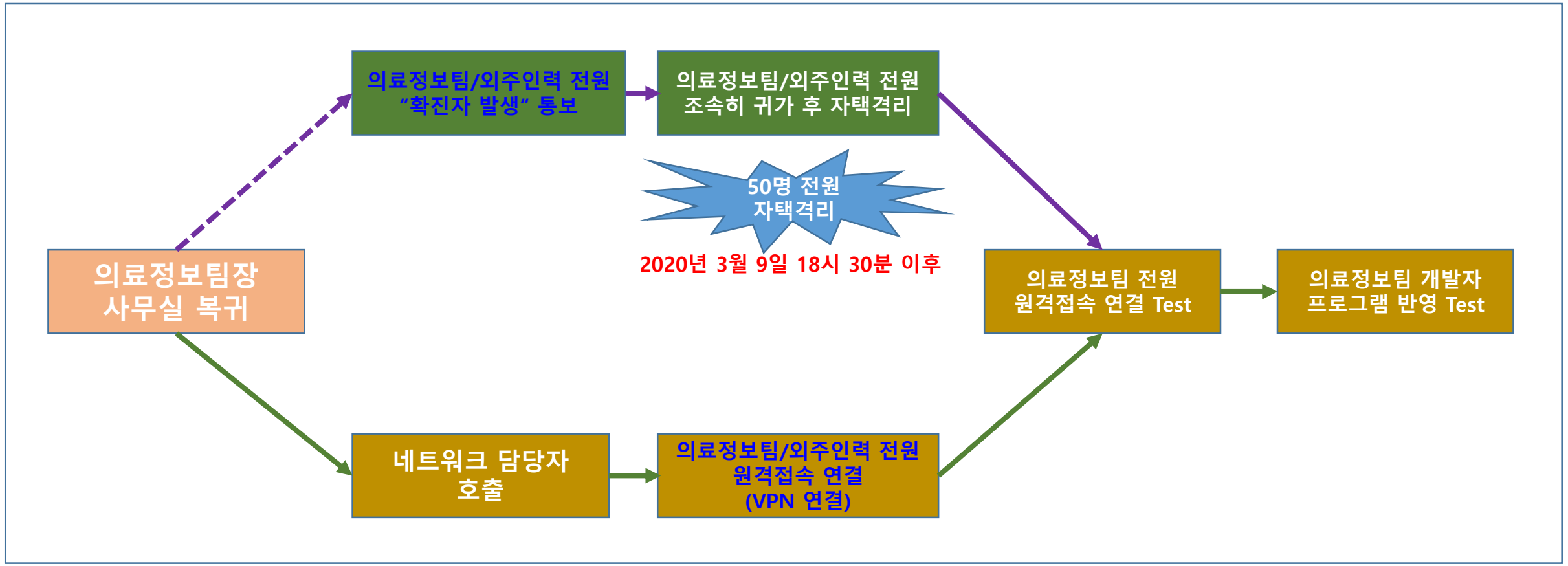
발표자 : 한기태(kthan@kuh.ac.kr)

1. 감염자 발생 및 원격지원 준비

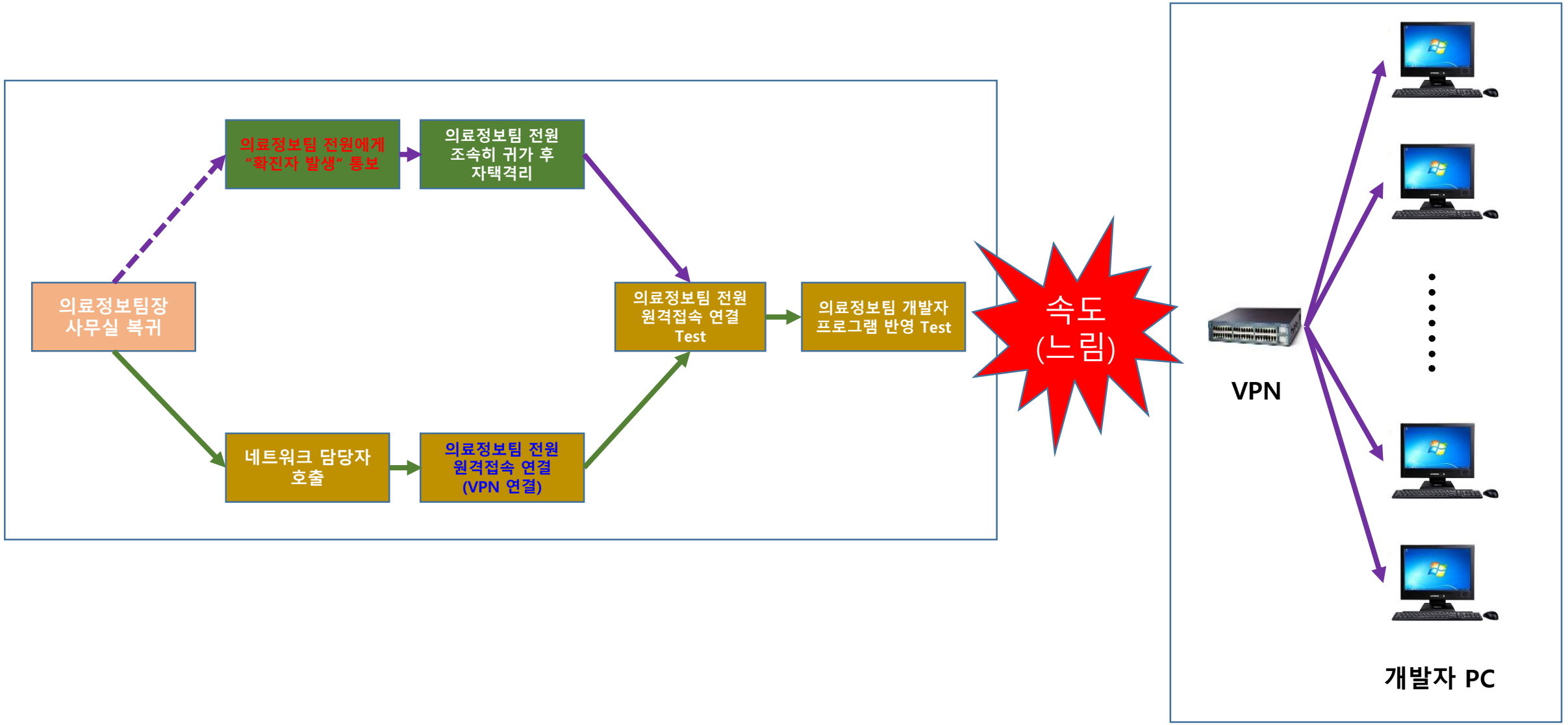
1. 감염자 발생 및 원격지원 준비



1. 감염자 발생 및 원격지원 준비

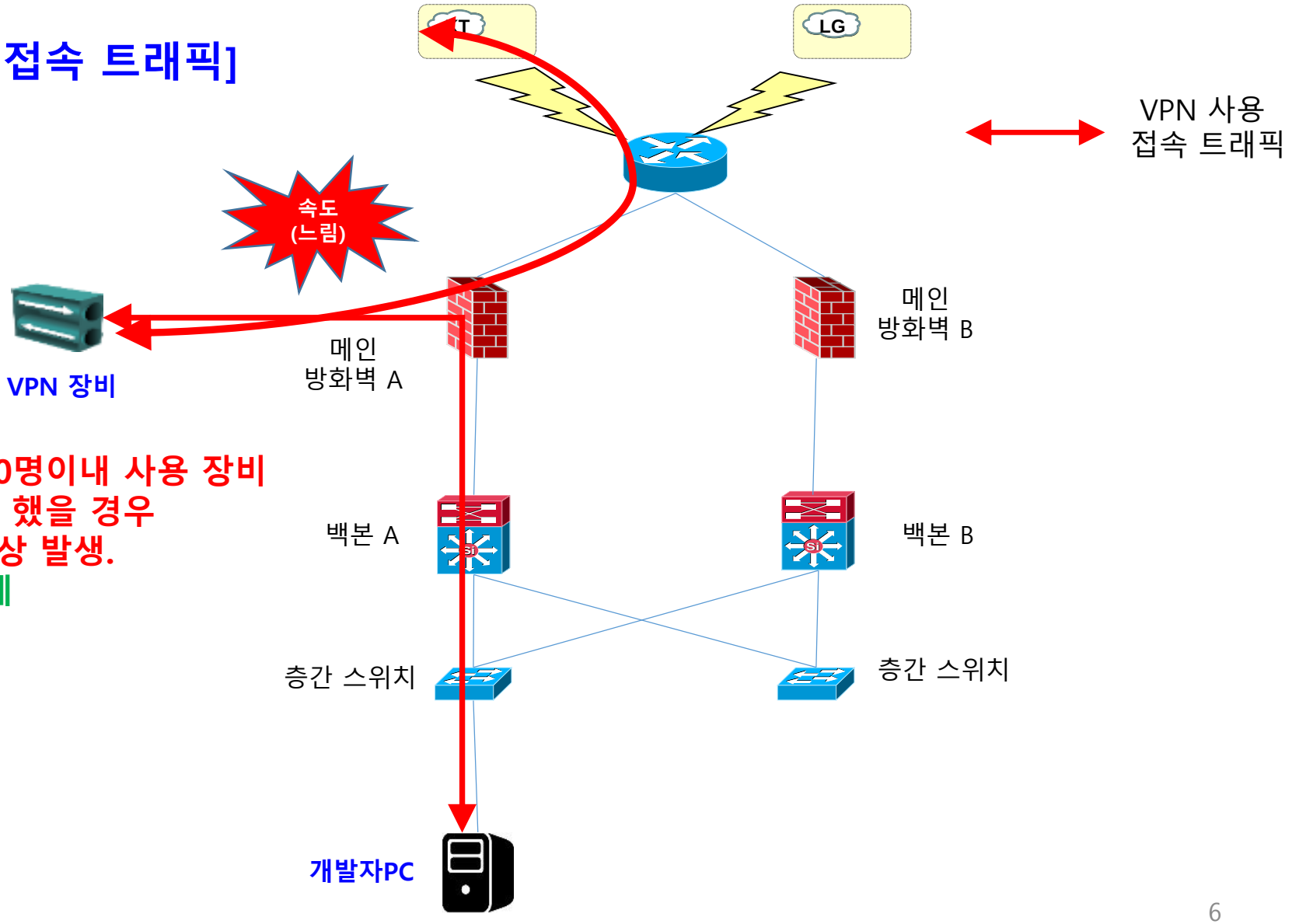


1. 감염자 발생 및 원격지원 준비



1. 감염자 발생 및 원격지원 준비

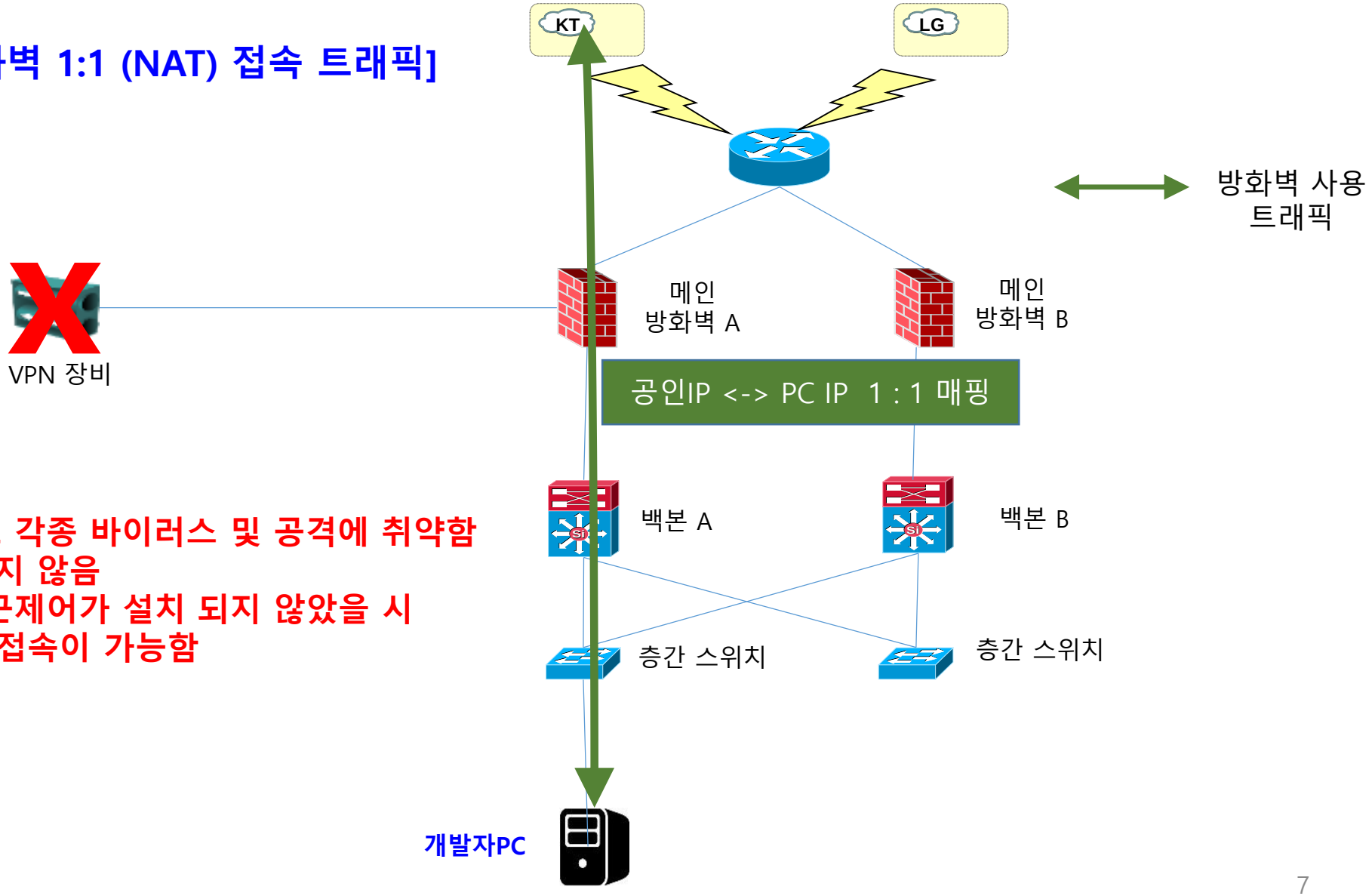
[의료정보팀 자가격리 시 VPN 접속 트래픽]



기존 VPN 장비 : 동시 접속자 최대 50명이내 사용 장비
10명이상 동시 접속 했을 경우
끊김과 느려지는 현상 발생.
-> VPN 성능의 문제

1. 감염자 발생 및 원격지원 준비

[의료정보팀 자가격리 방화벽 1:1 (NAT) 접속 트래픽]

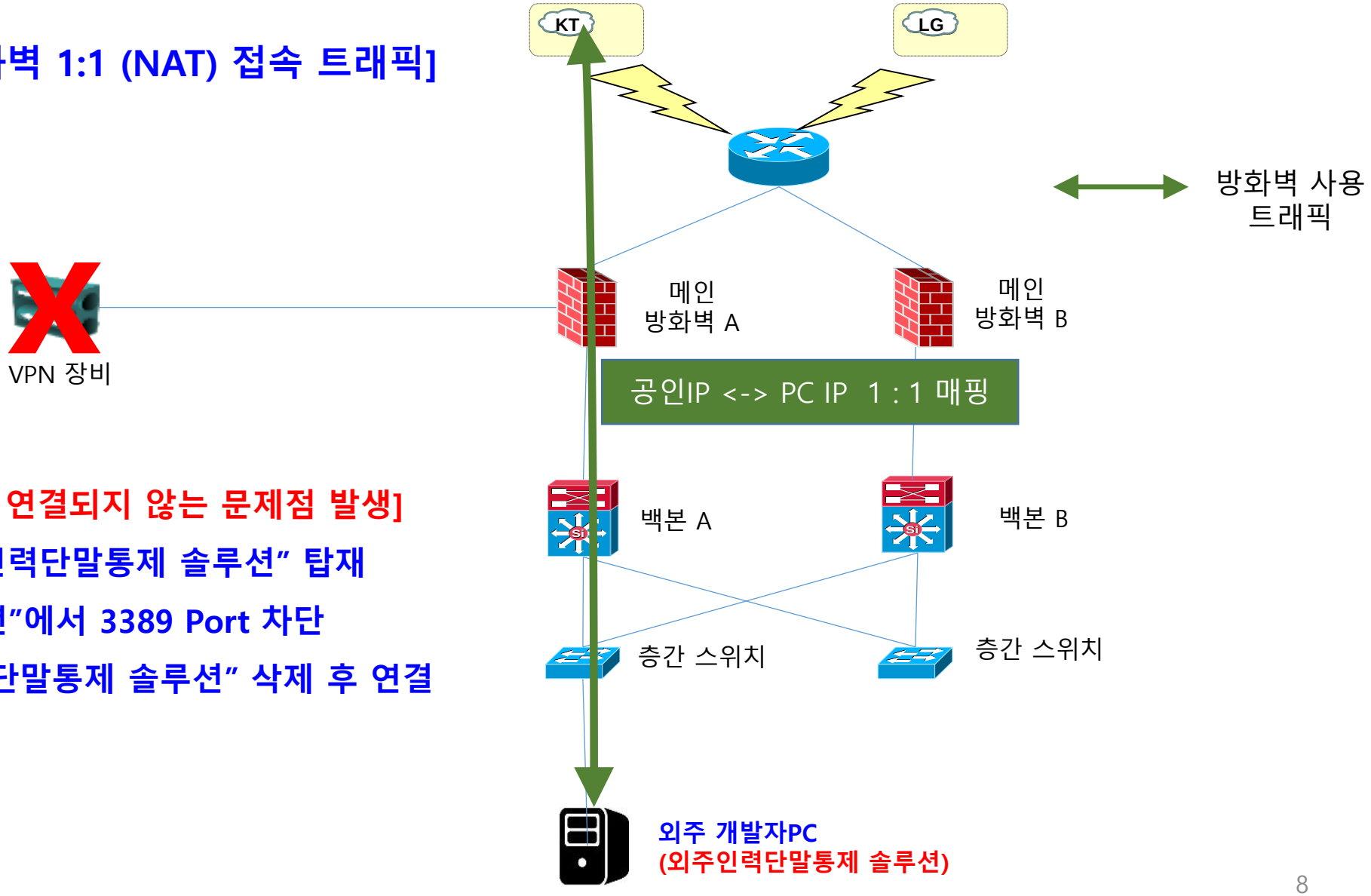


[1:1(NAT) 시 문제점]

가) 공인 IP 의 외부 노출로 각종 바이러스 및 공격에 취약함
나) 사용자 접속 로그가 남지 않음
다) 서버 접근제어, DB 접근제어가 설치 되지 않았을 시 서버존의 모든 장비로 접속이 가능함

1. 감염자 발생 및 원격지원 준비

[의료정보팀 자가격리 방화벽 1:1 (NAT) 접속 트래픽]



[1:1(NAT) 시 외주개발자 PC 연결되지 않는 문제점 발생]

- 외주 개발자 PC에 “외주인력단말통제 솔루션” 탑재
- “외주인력단말통제 솔루션”에서 3389 Port 차단
- 관리자 모드로 “외주인력단말통제 솔루션” 삭제 후 연결

1. 감염자 발생 및 원격지원 준비

[재택근무 환경 개선방안]

방안	세부 내용
VPN 장비	VPN 장비 성능 개선 (고성능으로 교체)
전용 솔루션	원격근무 전용 솔루션 도입 (클라우드 용 등)

1. 감염자 발생 및 원격지원 준비

[NAT 연결 후 자택 격리]

2020년 3월 9일 22시 30분

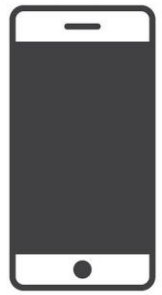
2. IT부서 전원 재택근무

[업무의 연속성 유지 -> 필수]

원내전화

착신 변경

IT부서
업무별 담당자 전화



업무별 담당자
휴대 전화

2. IT부서 전원 재택근무

[IT부서 물리적 보안]

[방역 팀]

[접근 불가]

[제3의 장소]

보안카드
비상출입키 관리대장

[IT 부서 직원 전원 자가격리]

[IT 부서 사무실]

[방역 구간 : 2차 소독]

[서 버 실]

[방역 제외 구역]

[출입구 CCTV]

2. IT부서 전원 재택근무

[IT 부서 소독]

2. IT부서 전원 재택근무

[업무의 연속성 유지]

	자가격리 1일차	자가격리 2일차	자가격리 3일차
인프라 Part	1차 소독 사무실 폐쇄	2차 소독 사무실 폐쇄	입실 허가(보건소) [유지보수 인력 상주] - 서버 담당자 1명 - DB 담당자 1명 - 네트워크 담당자 1명
개발 Part	전화 착신 (사내전화 -> 휴대전화) 재택 근무		

2. IT부서 전원 재택근무

[감염관리 행정 지원]

1. 자료 제출
   - 확진자 병원이동 동선 작성
   - 자가격리 대상자 병원이동 경로 작성
   - 외부직원 출입자 현황 작성
   - 확진자 및 자가격리자 원내 접촉자 현황 작성
   - 출입문 CCTV 영상 제공

2. 코로나 검사 현황 : 자가격리자
   - 검사현황 작성
   - 검사결과 작성
   - 자가격리 기간 현황 작성 (지차체 보건소 별 기준이 다름)

3. IT부서 재택근무 현황

[전산 개발 및 적용 규정 : 자가격리 기간]

자가격리 전산개발 규정	"자가격리 전산개발 규정" 운영
1. 프로그램 오류 수정	규정 준수
2. Data Base 자료(데이터) 확인	규정 준수
3. 신규 개발프로그램 반영 금지	응급 개발 프로그램 반영 코로나 관련 프로그램 개발 반영 (단 : 충분한 테스트 후에 반영)

3. IT부서 재택근무 현황

[인프라 업무 규정 : 자가격리 기간]

1. 시스템 모니터링
   - 서버 모니터링 : WEB, WAS, PACS, 의료장비 I/F 등
   - 네트워크 모니터링
   - Data Base 모니터링
   - 보안 솔루션 모니터링
   -> 매일 8시 30분 모니터링 후 보고
2. H/W 장애 발생
   - 서버실 폐쇄기간 : 방호복 착용 후 교체
   - 서버실 접근 허용 : 유지보수 업체 상주 인력이 H/W 교체

3. IT부서 재택근무 현황

[자가격리 기간 중 재택근무 후기]

1. 전산 개발

- 업무 협의가 원활하지 못하다.
- 장시간 원격접속 할 경우 네트워크가 끊어지는 경우 발생
- 프로그램 개발 및 수정 반영은 가능하다.
- 데이터 확인은 가능하다.

-> 결론 : 재택근무 가능하나, 업무 분석 단계에서 사용자간의 업무 협의는 원활하지 못함

2. 인프라 운영

- H/W 장애 발생 시 조치가 어렵다.
- H/W 성능저하 시 튜닝은 가능하다.

-> 결론 : 재택근무 불가능

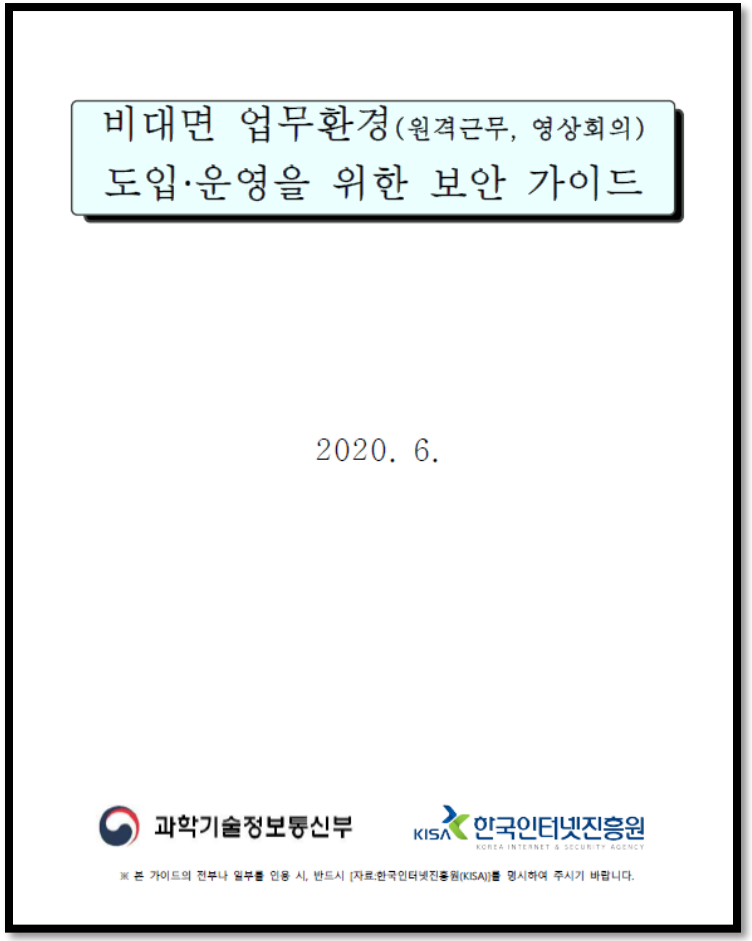
3. IT부서 재택근무 현황

[자가격리 기간 중 재택근무 후기]

3. 보안 : 가장 큰 위험

병원 내 자료유출 위험이 있다.

[참조]

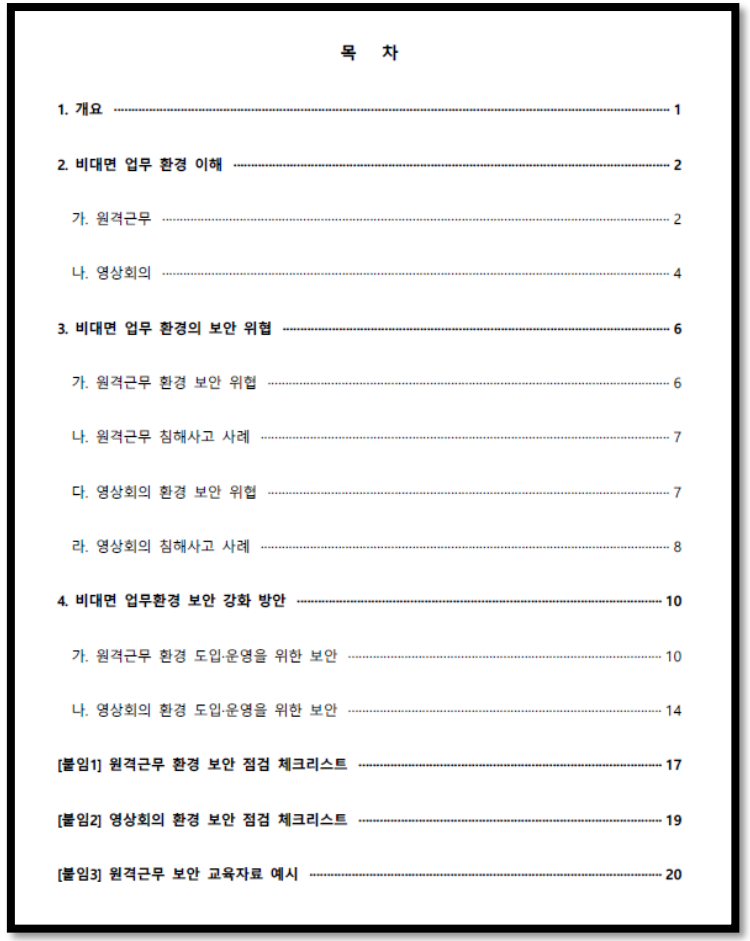


비대면 업무환경(원격근무, 영상회의)
도입·운영을 위한 보안 가이드

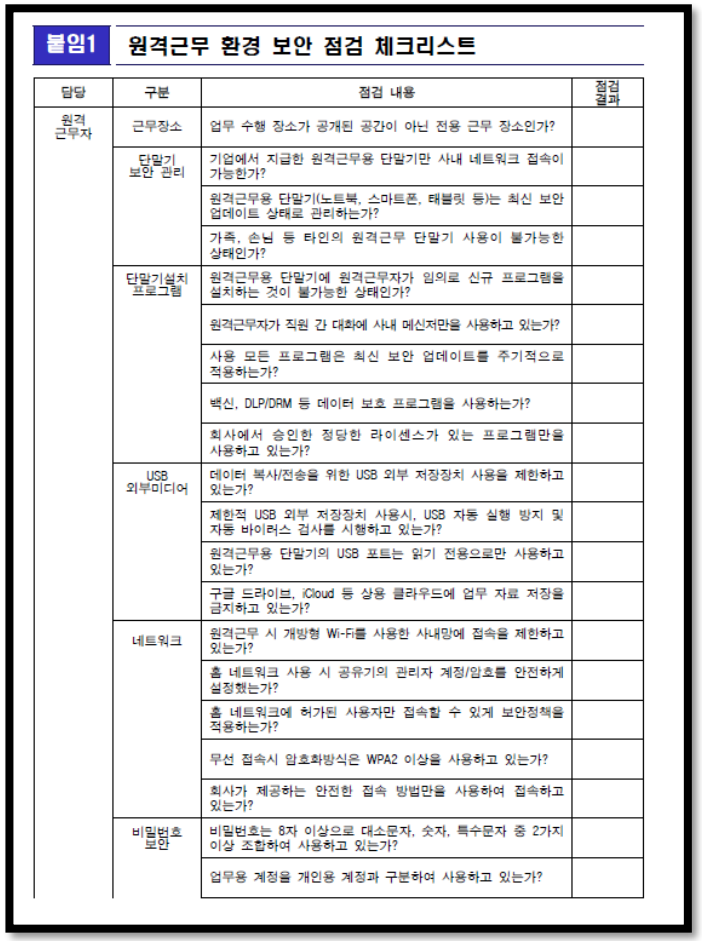
2020. 6.

과학기술정보통신부 KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY

※ 본 가이드의 전부나 일부를 인용 시, 반드시 [자료:한국인터넷진흥원(KISA)]를 명시하여 주시기 바랍니다.



목 차



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?	

경청해 주셔서 감사합니다.