

# 언택트 시대와 정보보호산업 촉진



글 메가존클라우드 차원호 매니저

## 언택트 시대와 정보보호산업 촉진

### 코로나19 확산과 근무환경 변화

코로나19가 전 세계적으로 확산됨에 따라 언택트 즉, 비대면 환경도 함께 확산되고 있다. 근무환경 역시 이러한 변화에 따라 정해진 사무공간에서 업무를 하던 기존 방식에서 재택근무 등 비대면이 가능한 환경에서 업무 할 수 있는 방향으로 급속히 변화하고 있으며, 많은 기업에서 이미 진행 중이거나 도입을 준비 중이다.

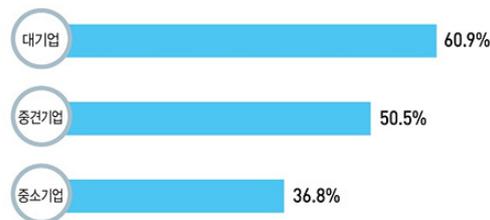
기업 규모별 재택근무 시행 비율을 살펴보면 대기업이나 중견기업 경우, 절반이 넘는 각 60.9%, 50.5%기업에서 재택근무를 시행 중이고, 중소기업의 경우 36.8%의 기업이 재택근무를 시행 중이다.



기업 규모별 재택근무 시행 비율을 살펴보면 대기업이나 중견기업 경우, 절반이 넘는 각 60.9%, 50.5%기업에서 재택근무를 시행 중이고, 중소기업의 경우 36.8%의 기업이 재택근무를 시행 중이다.



### 기업 규모별 재택근무 시행 비율



출처: 사람인(089개 기업 대상 설문)

### 디지털 전환에 따른 정보보호 이슈

이런 변화가 가능하게 된 중심에는 전통적인 ICT(정보통신기술) 기술과 인공지능(AI) 및 사물인터넷(IoT), 클라우드(Cloud), 빅데이터(Big Data), 모바일(Mobile)이 결합된 지능정보기술이 있으며 이런 기술들에 힘입어 많은 분야에서 디지털 전환을 이룰 수 있었다.

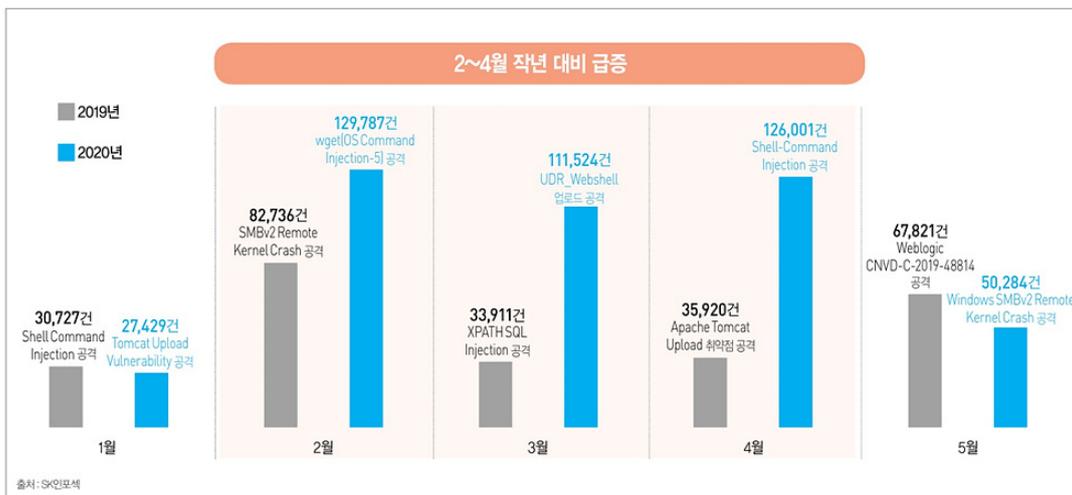
하지만 이러한 디지털 전환에 따라 사이버 공격 면(attack surface)도 확대가 된다. 어느 정도 보안의 경계가 가시적이었던 예전과는 달리 사용자, 설비, 사물, 인프라 등이 모두 연결된 디지털화된 산업 생태계는 보안 위협에 노출되는 취약점도 그만큼 증가했다.

안랩, 포티넷 등 다수의 보안 업체에서 발표한 2020년 보안 위협 전망에서는 디지털 전환에 따라 보안 취약점이 증가하였으며 공격 파괴력도 증가할 수 있다는 점을 강조하고 있다. 또한 사이버 보안 및 데이터 보안 업체인 탈레스가 발표한 '2019년 탈레스 데이터 위협 보고서'에 따르면 조사한 대다수(86%)의 기업이 데이터 위협에 취약한 것으로 나타났고, 30% 미만의 응답자만이 디지털 트랜스포메이션 전략의 일환으로 암호화를 채택하고 있는 것으로 조사됐다. 이는 기업들이 디지털 전환을 가속화하고 있지만 그만큼 데이터가 노출될 가능성도 증가하고 있다는 방증이다.

### 코로나19로 인한 사이버 공격 증가

코로나19가 급격히 확산된 2~4월의 경우 주요 공격 건수가 작년 대비 급증했다. 보안업체인 팔로알토 네트워크스(Palo Alto Networks)가 발표한 내용에 따르면 올해 1~3월 사이 'covid', 'virus', 'corona'를 포함한 10만여 개의 도메인을 분석한 결과 4만 개 이상의 고위험 도메인 및 2천 개 이상의 악성 도메인이 있었으며 특히 2~3월 사이에는 악성 도메인이 560% 증가했다.

#### > 코로나19 관련 주요 사이버 공격 현황



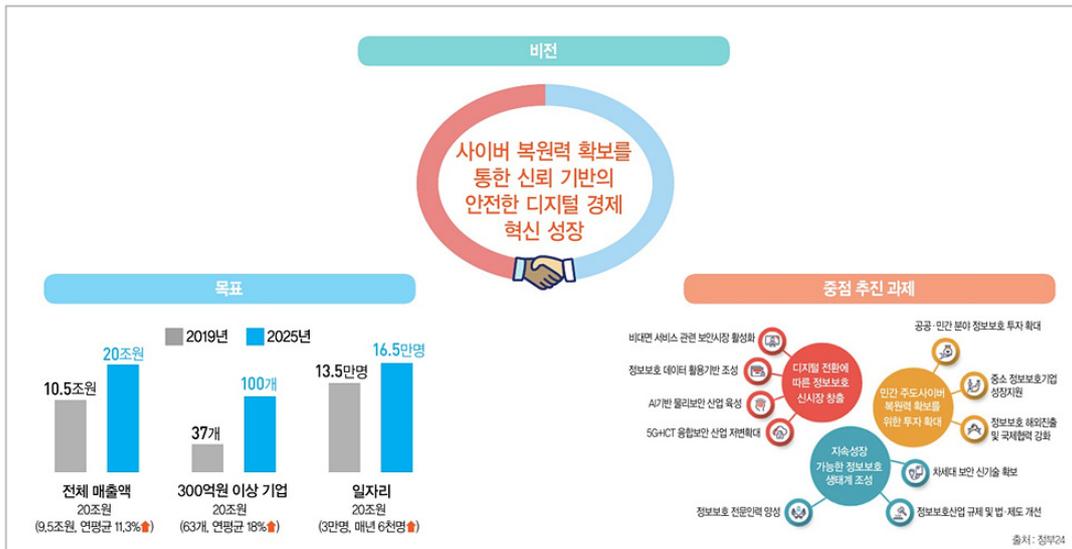
실제로 올해 봄 코로나19가 급속히 확산됨에 따라 화상회의 솔루션의 도입 및 활용이 폭발적으로 늘어날 때 화상회의 솔루션 중 하나인 '줌의 보안 취약점'을 노린 공격이 발생했다. 접속 링크가 포함되어 있는 초대장만 있으면 누구나 회의에 참석할 수 있다는 취약점을 이용한 방법으로 제 3자가 화상회의에 들어와서 정치적 메시지나 폭력적인 행위, 인종 차별 발언 등을 하는 줌 폭탄(Zoom Bombing) 문제가 발생하였으며 이로 인해 회의나 줌을 통한 교육 등이 취소되는 일이 종종 발생했다. 여기에 더해 데이터가 중국에 있는 서버를 경유한다는 사실이 밝혀져 개인정보 유출 가능성이 제기되기도 했다.

### 제2차 정보보호산업 진흥계획

국내 정보보호산업의 경우 제1차 산업진흥계획을 통해 2019년말 국내 정보보호 시장 10.5조 돌파, 정보보호 기업의 수는 2016년 대비 230개 증가 등 양적 성장을 이루었으나 디지털 전환과 비대면 서비스의 확산에 따라 기존 정보보호의 패러다임 변화가 시작됐다. 회사 사내망 내부 보안에 중점을 둔 환경이 회사 외부 근무가 증가함에 따라 보안점검 포인트가 변화한 것이다. 이에 과학기술정보통신부(이하 과기정통부)에서는 모든 산업의 디지털 전환과 비대면 사회 도래, D(데이터 Data)·N(네트워크 Network)·A(인공지능 AI) 기술 확산에 따라 신뢰 기반의 디지털 사회로 나가기 위한 방안의 일환으로 2021년부터 2025년까지 추진될 범정부 차원의 법정계획인 '제2차 정보보호산업 진흥계획'을 수립했다.

2차 진흥계획은 정보보호산업 전체 매출액 20조원, 300억 매출액 이상 기업 100개, 일자리 16만 5,000명 3대 목표와 디지털 전환에 따른 정보보호 신시장 진출, 민간 주도 사이버 복원력 확보를 위한 투자 확대, 지속성장 가능한 정보보호 생태계 조성 등 3가지 주요 육성 전략을 기반으로 한 10대 중점 추진 과제를 담고 있다.

#### > 제2차 정보보호산업 진흥계획

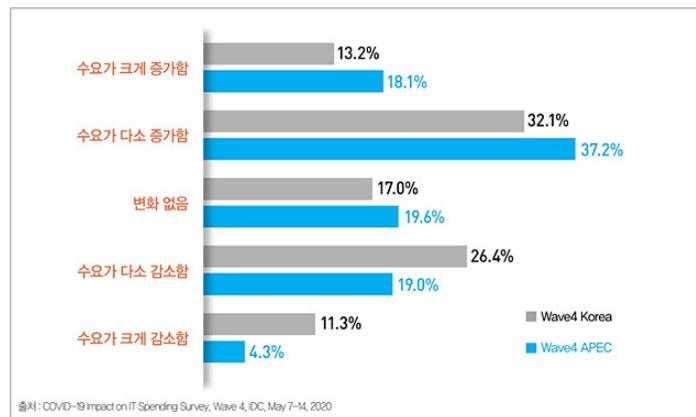


### 안전한 클라우드 사용을 위한 클라우드 보안인증제

비대면 기반 디지털 전환이 가능해진 주요 기술의 중심에는 클라우드가 있다. 고정된 장소 또는 환경에서만 접근이 가능했던 기존 디지털 환경에 비해 클라우드를 사용하면 언제 어디서나 접근이 가능하다.

최근 코로나19 확산으로 인하여 기업들의 클라우드 수요가 증가하였으며 이는 비대면이 만연한 뉴노멀 시대 기업들의 대응에 있어 클라우드의 역할을 중요하게 인식하고 있다고 볼 수 있다.

#### ▶ 코로나19 여파에 따른 클라우드 컴퓨팅 투자수요 변화



“ 최근 코로나19 확산으로 인하여 기업들의 클라우드 수요가 증가하였으며 이는 비대면이 만연한 뉴노멀 시대 기업들의 대응에 있어 클라우드의 역할을 중요하게 인식하고 있다고 볼 수 있다. ”

클라우드에 대한 수요가 증가함에 따라 안전한 클라우드 사용을 위한 클라우드 보안에 대한 요구도 증가하고 있다. 국내에서도 한국인터넷진흥원(이하 KISA)에서 클라우드 보안인증제를 시행하여 이용자들이 안심하고 클라우드 서비스를 이용할 수 있도록 지원하고 있으며 동 기관에서 시행하는 정보보호 및 개인정보보호 관리체계(이하 ISMS-P)의 요구사항에도 클라우드 보안 항목을 포함하고 있다.

아마존웹서비스(AWS)나 마이크로소프트의 클라우드 서비스 애저(Azure) 등 국내에 진출한 글로벌 클라우드 사업 기업들 역시 이러한 클라우드 서비스 보안 강화 및 안전한 클라우드 서비스 제공을 위하여 정보보호관리체계 인증 제도(이하 ISMS)를 획득하였으며 국내 클라우드 MSP 역시 ISMS 또는 ISMS-P를 획득하고 있다.

이 중 클라우드 보안인증제는 공공기관이 안전하게 민간 클라우드를 이용할 수 있도록 서비스 제공자가 제공하는 서비스에 대해 정보보호 기준의 준수여부 확인을 인증기관이 평가·인증하여 이용자들이 안심하고 클라우드서비스를 이용할 수 있도록 지원하는 클라우드에 특화된 제도이다. 따라서 클라우드 보안인증 신청기관은 공공기관의 업무를 위해 클라우드서비스를 제공하려는 클라우드서비스 제공자가 되며, 클라우드 보안인증 평가·인증대상은 클라우드서비스를 이용하여 정보 시스템의 인프라(IaaS), 응용프로그램(SaaS), 개발환경(PaaS) 중 어느 하나 이상을 제공하는 클라우드서비스가 해당된다. 평가·인증 범위를 보면 클라우드서비스에 직접 포함이 되어 있거나 관련된 자산, 조직, 지원서비스 등을 모두 포함하여 서버,

네트워크 등의 장비부터 문서, 설비, 가상자원, 응용 프로그램, 모니터링, 로그 분석 등에 이른다.

클라우드 보안인증제는 클라우드서비스 유형에 따라 다른 통제항목이 적용된다. 통제항목은 보안의 기본 요소인 관리적·물리적·기술적 보호조치 및 공공기관용 보호조치로 구성되며 IaaS 표준등급의 경우 총 14개 분야 117개 통제항목으로 구성되지만 PaaS, SaaS 표준등급의 경우 총 13개 분야 78개 통제항목(SaaS 간편등급의 경우 11개 분야 30개 통제항목)으로 구성된다.

SaaS 서비스의 경우 기본적으로 클라우드서비스 보안인증을 받은 IaaS 서비스 환경에서 구축이 되어야 하므로 IaaS보다 적은 수의 통제항목으로 구성된다. IaaS·PaaS·SaaS 표준등급은 유효기간이 5년, SaaS 간편등급은 유효기간이 3년으로 최초평가 후 매년 1회 이상 사후평가를 거쳐 유효기간 만료 전 인증을 연장하려면 갱신평가를 받아야 한다. 갱신평가 후에는 다시 유효기간이 3~5년으로 연장된다.

> 클라우드서비스 보안인증제 안내서(2019.11)

구분	IaaS 인증	SaaS 인증		PaaS 인증
	표준등급	표준등급	간편등급	표준등급
인증항목	117개	78개	30개	78개
유효기간	5년	5년	3년	5년

출처: 한국인터넷진흥원(KISA)

근무환경 변화에 따른 보안 위협

업무특성 상 원격 근무가 어려웠던 금융권에서도 재택근무 등을 통해 업무 연속성을 유지할 수 있도록 '비조치 의견서' 회신으로 조치했다. 이러한 근무환경의 변화로 정보보호산업에 대한 수요는 계속 증가할 것으로 보인다. 재택근무가 증가하면서 많은 기업들이 필수적으로 가상 사설망(이하 VPN)을 활용하여 외부에서 기업 내부 자원으로서의 접근을 통제하고 있다. VPN 접속이 이루어지는 PC 측, 엔드포인트 보안을 위해 보안 프로그램을 이용하여 최신 보안 업데이트 확인, 외부 저장 장치로 데이터 전송, 화면 캡처 등 필요에 따라 통제 및 관리를 한다. 또한 문서암호화(DRM), 정보유출방지(DLP) 등의 솔루션을 함께 이용하여 보안을 강화하는 경우도 많으며 클라우드 기반의 SaaS 서비스의 경우 해당 기능들을 함께 제공해 주는 서비스들도 있다. VPN 접속 시에도 이중 인증 절차(2FA)를 거쳐 보안을 강화한다. 또한 접근 통제와 함께 로그 분석을 통하여 인증, 주요 데이터 접근 등 온라인 상에서 이루어지는 행위 중 이상 행위 탐지도 함께 요구하는 경우가 증가하고 있다.

이러한 개별 관리의 어려움으로 인하여 일부 기업에서는 데이터센터나 클라우드상에 구축한 데스크톱 가상화(VDI) 서비스를 이용하여 업무 환경을 가상화해 중앙에서 통제 가능한 보안이 강화된 환경에서 업무를 진행할 수 있도록 하는 경우도 증가하고 있다. 사용자 입장에서는 모든 데이터가 중앙에 저장되고 관리되므로 데이터 유출 및 손실에 대한 걱정을 덜 수 있는 장점이 있다.

외부에서의 접속이 증가할수록 이에 따른 취약점을 노리는 디도스(DDoS) 공격, 메



“ 재택근무가 증가하면서 많은 기업들이 필수적으로 가상 사설망(이하 VPN)을 활용하여 외부에서 기업 내부 자원으로서의 접근을 통제하고 있다. ”

일을 이용한 피싱, 랜섬웨어 공격 등 수많은 보안위협이 발생할 가능성도 함께 증가하기 때문에 이에 대한 철저한 대비가 필요하다.

### SIEM을 보완하는 보안 운영 자동화 및 대응

보안 위협은 나날이 증가하지만 이를 대처할 수 있는 보안 인력은 부족한 상황에 보안 관제의 효율성은 높이고 복잡성은 낮출 수 있는 보안 운영 자동화 및 대응(Security Orchestration, Automation and Response, SOAR) 기술이 더욱 주목을 받고 있다.

많은 기업들이 보안 시스템을 도입하고 여기에서 쏟아지는 막대한 로그를 중앙에서 관리·분석하여 위협을 탐지할 수 있도록 SIEM(Security Information and Event Management)을 도입했다. 최근에는 AI, 내부자 위협에 대한 보호를 위한 사용자 및 계정 행위 분석(User and Entity Behavior Analytics, UEBA) 등의 기술을 접목하여 보다 강력해진 차세대 SIEM으로 거듭 진화하고 있다.

그러나 이에 따라 탐지 및 분석 과정이 많아졌을 뿐만 아니라 위협에 대응이 어려운 부분이 존재한다. SIEM이 발전을 하더라도 보안관제 업무는 관제인력의 숙련도와 전문성에 달려 있으나 보안 인력은 크게 부족한 상태이다.

지금은 규제 효력이 사라졌지만 금융권의 IT·정보보호(보안) 인력과 예산에 관한 권고 기준에는 일명 '5·5·7' 기준이 있었다. 이는 IT인력을 전체 인력의 5% 이상, 전체 IT 인력 가운데 보안인력은 5% 이상, 보안예산은 전체 IT예산 중 7% 이상 각각 확보해야 한다는 내용이다. 하지만 현실은 IT인력이 100명이 있더라도 이 중 보안인력은 5명에 불과하다. 이렇듯 기술과 솔루션은 날로 복잡해지지만 보안인력은 부족을 해결하고자 SOAR가 등장했다.



“ 많은 기업들이 보안 시스템을 도입하고 여기에서 쏟아지는 막대한 로그를 중앙에서 관리·분석하여 위협을 탐지할 수 있도록 SIEM(Security Information and Event Management)을 도입했다. ”



출처: 가트너

SOAR는 2017년 가트너에서 만든 용어로 다양한 보안 위협의 대응 프로세스를 자동화해 가능한 사람의 개입없이 보안 침해 사고에 대응하고 인력의 개입이 필요한 사고 발생시 표준화되어 있는 업무 프로세스에 따라 직원이 보다 쉽게 높은 수준의 위협에 대응할 수 있도록 도와주는 보안 자동화 플랫폼이다.

SOAR는 보안 오케스트레이션 및 자동화(Security Orchestration and Automation, SOA), 보안 사고 대응 플랫폼(Security Incident Response Platform, SIRP), 위협 인텔리전스 플랫폼(Threat Intelligence Platform, TIP)의 세 가지 핵심 기능으로 구성된다.

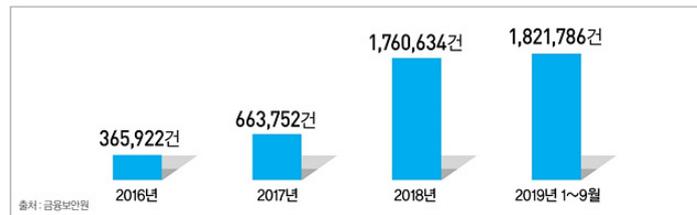
SOA는 보안 관제팀이 위협을 선별, 조사 및 완화하기 위해 사용하는 도구들을 통합 관리하고 플레이북(특정 작업 절차 표준화)을 생성하고 도구들 간 업무흐름을 자동화한다.

SIRP는 보안 사고 발생 시 대응 체계의 자동화로 R&R, 필요한 조치 사항, 해결이 되어야 하는 시간 등을 관리한다. TIP는 다양한 소스에서 실시간으로 위협 데이터를 수집하고 분석하여 보안 위협을 대응할 수 있도록 도움을 준다.

### 금융권 보안투자 현황

금융계열사는 다양한 산업군 중 대표적인 사이버 공격 대상이면서 보안에 가장 민감한 그룹 중 하나다. 금융보안원에 따르면, 금융권 대상 사이버 공격은 해가 갈수록 점점 증가하고 있다. AI, 머신러닝 등을 활용한 지능화 및 통합화를 이용한 선제적 대응을 통해 기존의 보안 체계를 고도화하려는 움직임을 보이고 있다.

#### > 금융권 연도별 사이버 공격 대응건수



먼저 BNK부산은행은 2017년부터 3년간 독자적인 정보보호 통합 플랫폼을 구축 및 고도화 작업을 진행해왔으며 현재 ETIR 모델을 구성하는 각 영역에 부합한 SOAR 보안관제시스템을 구현, 통합 정보보호 플랫폼의 핵심 요소로 활용하고 있다. 올해는 망연계구간의 지능형지속보안위협(Advanced Persistent Threat, APT) 보안을 한층 더 강화했다.

NH농협은행은 국내 은행권 최초로 단말이상행위탐지시스템(Endpoint Detection & Response, EDR) 구축사업을 진행하여 지난해 EDR 1차 시범사업을 통해 영업점 4000대에 PC에 대한 EDR 구현을 마쳤으며, 올해 2단계를 추진한다. 또한 보안분야에는 2022년까지 32개 추진 과제를 선정하였고 이 중 9개 과제를 올해 완료할 예정이다. 올해의 과제 중에는 2022년까지 완료를 목표로 하는 '보안관제 대응체계 SOAR 구축'도 포함되어 있어 SOAR에 대한 검토 및 사전분석, 컨설팅을 진행할 예정이다.

우리은행은 머신러닝 기술을 활용한 예측형 통합관제시스템을 구축해 보안 위협에 대응하는 전략이다. KB국민은행도 올해 3월에 오픈한 '신(新) 모니터링 시스템'을 통해 금융소비자의 금융거래 패턴과 자금 흐름 등을 실시간으로 분석해 보이스피싱 징후를 탐지하고 있으며 향후 수집된 정보와 IT기술을 결합해 보이스피싱 사기 거래에 대한 탐지율을 향상시키는 등 보이스피싱 거래의 원천 차단을 위한 예방 시스템 구축을 지속해 나간다는 방침을 가지고 있다. 이렇듯 금융계열사는 언택트 시대에 클라우드 확장 및 이에 맞춰 신규 보안 시스템 구축 또는 기존 보안 시스템 고도화에 투자를 늘려 나가고 있다.

다음 페이지에서 '언택트 시대 정보보호' 관련 인포그래픽을 한눈에 보실 수 있습니다.

Infographics

언택트 시대 정보보호 관련 정보 한눈에 보기

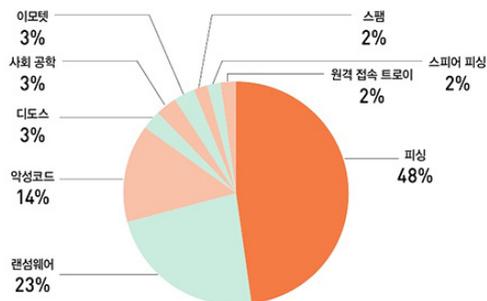
> 제2차 정보보호산업 진흥계획 중점 추진 과제



> 2020년 상반기 보안위협 TOP5



> 코로나19 관련 사이버 공격 현황



> 사이버 공격 발생 통계(건)

구분	1월	2월	3월	1분기 평균
2020년	566,872	556,033	624,986	582,630
2019년	548,141	335,502	560,776	481,473

출처: SK인포섹 사큐디움 센터

▶ 주요 금융회사 등의 재택근무 방안 등 사례

구분	재택근무 방안 등 사례
씨티은행	대체근무지 시설 점검, 유사시 원격근무를 위한 권한신청 접수 등 진행
KB국민은행	전산센터 이원화 운영 중(여의도, 김포), IT 부문·자본시장본부 등은 분리근무 시행 중
신한은행	IT 업무 핵심인력 11개 대체사업장에 분산배치(서울 중구, 강남구, 영등포구, 일산, 죽전, 광고 등)
우리은행	남산타워, 서울연수원 등 대체 사업장 마련, 상황에 따라 대체사업장 가동 범위 확대
하나은행	인천 청라, 서울 중구 서소문 등에 대체사업장 마련-대체사업장 추가신설 논의 중
카카오뱅크	2.24부터 대체 사업장에서 근무 시작
케이뱅크	대체인력 운용 계획 수립, 유사시 대체사업장 운영
미래에셋	비상상황 대비 자금·결제·IT관련 부서 150여 명의 필수인력 확보
NH증권	비상상황 대비 자금·결제·IT관련 부서 150여 명의 필수인력 확보
KB증권	자금·결제·IT관련 부서 인력 분산 근무
한국투자신탁운용	본사 인력 중 약 16% 인력을 비상근무 대상으로 지정, 대체 근무지, 재택 분산 근무 실시
금융결제원	예방행동지침 전파, 시스템 운영 인력 등 분산 근무 실시, 비상 시 대체사업장, 재택근무
코스콤	비상근무인력 편성 완료, 원격접속 및 재택근무 환경 구축, 전산실 상황실 비상통제 체계 마련
금융보안원	금융보안원 본원 외 원격지(여의도 교육센터)에서도 24시간 보안 관제가 가능하도록 조치
에탁결제원	비상상황 발생 등을 고려해 재택근무 훈련 등을 실시

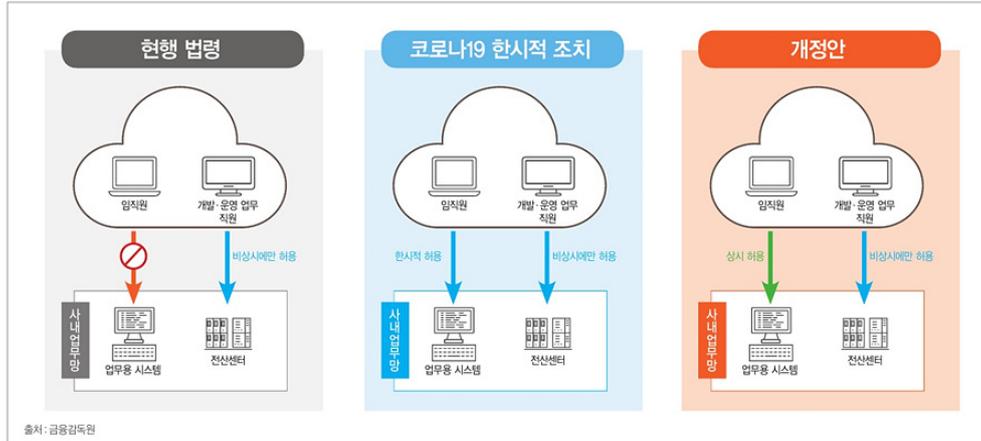
출처: 금융위원회

▶ 금융분야 사전예방 5대 수칙

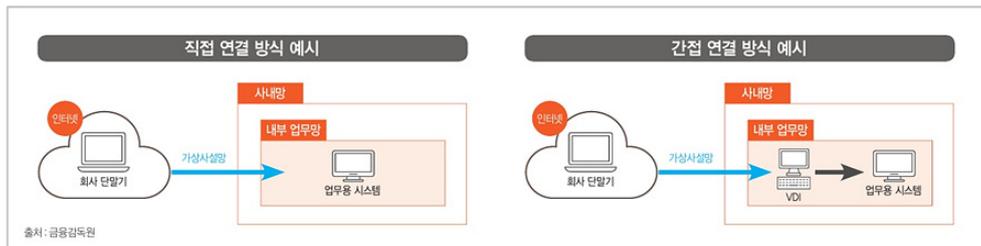
금융회사 감염예방 5대 수칙	금융이용자 안전이용 5대 수칙
<p>1  운영체제 및 사용 프로그램을 최신 버전으로 유지</p>	<p>1  모르는 사람이 보낸 이메일 첨부파일 실행 및 링크된 이미지 클릭 주의</p>
<p>2  최신 버전의 백신 프로그램 설치 및 주기적 업데이트</p>	<p>2  인터넷에서 출처가 불분명한 파일 다운로드 및 실행 금지</p>
<p>3  백신 실시간 탐지 활성화 및 주기적 검사 실행</p>	<p>3  금융당국 및 정부기관을 사칭하는 협박성 이메일 주의</p>
<p>4  웹브라우저 팝업 차단 기능 설정</p>	<p>4  신뢰할 수 없는 사이트 방문 자제 및 확인되지 않은 URL 클릭 주의</p>
<p>5  신뢰할 수 있는 정품 소프트웨어 사용</p>	<p>5  공식스토어(애플 앱스토어, 구글 플레이스토어) 이외 앱 설치 주의</p>

출처: 금융보안원

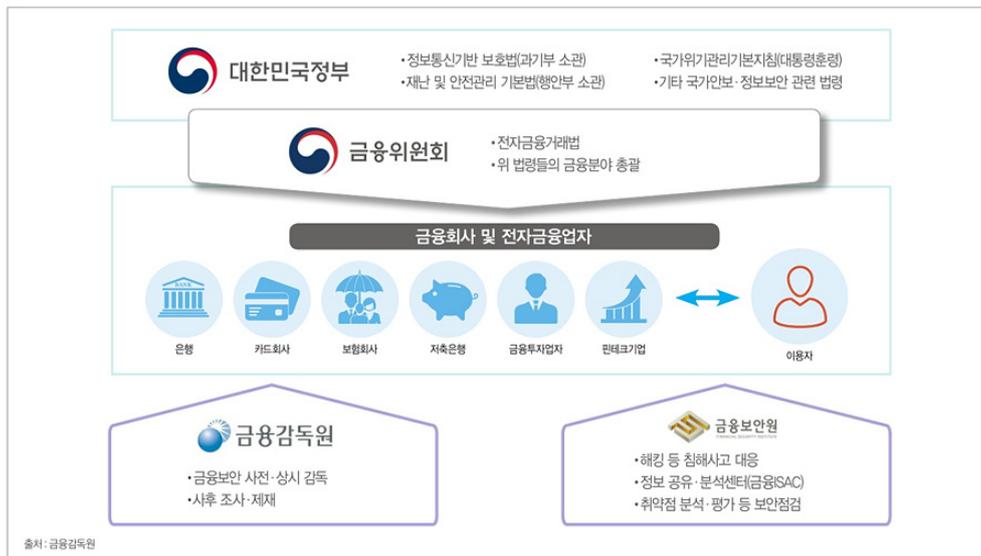
▶ 재택근무 관련 망분리 제도 개선사항



▶ 망분리 제도 개선 주요내용



▶ 금융분야 사전예방 및 위기관리 대응 체계



코로나19가 전 세계적으로 확산됨에 따라 언택트 즉, 비대면 환경도 함께 확산되고 있다. 근무환경

역시 이러한 변화에 따라 정해진 사무공간에서 업무를 하던 기존 방식에서 재택근무 등 비대면이 가능한 환경에서 업무 할 수 있는 방향으로 급속히 변화하고 있으며, 많은 기업에서 이미 진행 중이거나 도입을 준비 중이다.

- \* 저작권법에 의하여 해당 콘텐츠는 코스콤에 저작권이 있습니다.
- \* 따라서, 해당 콘텐츠는 사전 동의없이 2차 가공 및 영리적인 이용을 금합니다.

## 코스콤 큐레이션 박스 #코로나19

- \*. 포스트 코로나 시대, 클라우드의 부상
- \*. [카드뉴스] 포스트 코로나 시대, 언택트 이코노미와 금융 디지털 트랜스포메이션
- \*. [카드뉴스] 포스트 코로나 시대, 클라우드의 부상