정 보 보 호 학 회 지
제 31 권 제3호, 2021. 6

최근 사이버위협 동향과 가상사설망을 활용한 재택 근무자 보안 강화 기술 연구

강 동 윤*, 이 상 웅**, 이 재 우***, 이 용 준****

요 약

최근 코로나19 바이러스 감염병 유행으로 전 세계 다수 기업에서는 재택근무제도를 도입했다. 재택근무 경험자 중 절반 이상이 보안위협을 경험하였으며, 다수 기업에서는 자산정보를 보호하기 위해 사내 정보보안 강화에 더욱 중요해졌다. 재택근무를 하기 위해 근로자는 주로 가상사설망을 이용하여 업무를 수행한다. 재택근무제도의 활용도가 높아짐에 따라 재택근무 관련 사이버보안 위협은 증가하고 있다. 이러한 사이버 위협이 증가하고 있으며 가상사설망에서의 보안관제는 앞으로 매우 중요하다. 본 연구는 안전한 재택근무를 위해 가상사설망에서 발생하는 사이버위협에 대한 요소를 정리하여 효율적이고 체계적인 가상사설망을 활용한 보안 강화 방안에 대해 연구한다.

Ⅰ. 서 론

2019년 12월부터 최근까지 코로나19 바이러스 감염병이 지속적으로 확산되어 전 세계 다수 기업에서는 근로자의 안전과 업무의 연속성을 이어가기 위해 재택근무 제도를 도입하였다.

재택근무로 인해 효율적인 업무를 수행함과 동시에 비용 절감, 근로자의 휴식을 보장할 수 있는 장점이 있어 근로자의 만족도는 높아졌지만 급격한 재택근무 도입으로 사이버 보안에 대한 문제는 지속적으로 나타나고 있다.

한 언론에서는 코로나19 바이러스 감염병 확산으로 인해 보안업계도 비상상황이며, 이로 인한 재택근무의 확산은 보안업계의 과제로 다가왔다. 현장근무가 아닌 원격기술을 이용한 재택근무가 활성화되면서 이에 대응할 수 있는 보안 솔루션이 급격히 요구되고 있다. 이에 보안업계는 문서중앙화 클라우드 서비스, VPN 등을 다양하게 제안하고 있다. 또한, 이슈를 악용한 사이버 공격은 물론, 원격·재택근무 확대에 대한 보안 우려가 큰 점으로 확인되고 있다[1].

본 논문은 코로나19 바이러스 감염병 확산으로 재택근무 제도가 확대 시행되는 상황에서 가상사설망을 활용한 보안 강화 기술에 대한 연구이다.

Ⅱ. 관련연구

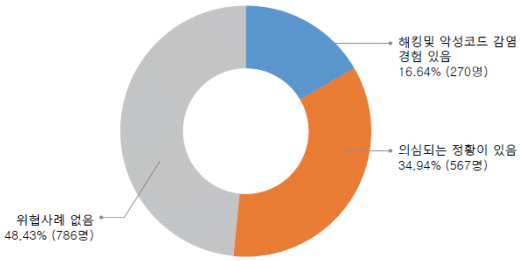
2.1. 사이버위협 동향 보고서

한국인터넷진흥원의 2020년 2분기 사이버 위협 동향 보고서 내용 중 아래 [그림 1]은 설문조사 항목으로 재택근무 간 근로자의 사이버 위협에 대한 설문조사이다.

설문조사 방법은 한국인터넷진흥원 SNS 이용자 대상으로 2020년 05월 18일부터 2020년 05월 22일까지 설문 참여자 2,250명을 대상으로 조사했다[2].

학생 외 비근로자를 제외한 재택근무를 경험한 응답자 1,623명 중, 해킹 및 악성코드 감염 경험 있음은 270명(16.64%)로 나타났으며, 의심되는 정황이 있었다고 응답한 수는 567명(34.94%)로 나타났다. 두 응답을 모두 포함한 37명(51.57%)는 중복 응답임을 고려하더라도 매우 높은 수준의 사이버 보안 위협 발생을 확인할 수 있다[2].

* 동국대학교 국제정보보호대학원 정보보호학과 (대학원생, nef4529@dgu.ac.kr)
** 동국대학교 국제정보보호대학원 사이버포렌식학과 (대학원생, sangwoong1293@dgu.ac.kr)
*** 동국대학교 국제정보보호대학원 정보보호학과 (석좌교수, jwlee0904@daum.net)
**** 극동대학교 해킹보안학과 (조교수, 2020032@kdu.ac.kr)



〔그림 1〕 재택근무 시 보안 위협 경험〔2〕

재택근무 시 사이버 보안 위협에 대해 매우 높은 수준 인 만큼 사이버 동향 보고서에도 2020년 4월 원격·재택근무 확대에 따른 사이버 보안위협이 다수 게시되었다.

2.2. 2021 국가정보보호백서

2.2.1. 2020년 정보보호 10대 이슈

국가정보원 외 다수 국가행정부처에서 발간한 2021 국가정보보호백서에서 2020년 정보보호 10대 이슈 중 “코로나19 팬데믹으로 인한 비대면 사회로의 진입과 사이버보안의 중요성”이 선정이 되었다.

코로나19 팬데믹은 일상 전반의 고도화 된 디지털 전환을 앞당기고, 경제 및 교육 등 중요하고 일상적인 활동을 비대면 중심으로 변화하는 계기가 되었다. 그러나 사이버 위협에 준비되지 않은 상태에서 재택근무, 원격교육, 화상회의, 온라인 상업활동 등 온라인 플랫폼을 활용한 비대면 중심의 활동이 급격히 증가하였다.

이에 따라 상대적으로 보안에 취약한 가정용 장비, 네트워크, 원격장비, 화상회의 플랫폼 등을 대상으로 하는 사이버 공격이 증가하였다. 즉 코로나19 팬데믹은 사이버 공격의 새로운 대상과 범위를 일상 전반으로 확대 및 심화하였다[3].

현재의 비대면 중심의 문화가 코로나19 팬데믹 종식 이후에도 앞으로 미래에 지속될 것으로 전망한다. 또한 5G, 사물인터넷(IoT), 클라우드 등 디지털 신기술의 고도화 및 지능화 된 발전과 도입이 가속화되면서 그 동안 제기되었던 사이버 보안 이슈가 더욱 심화될 것으로 전망하기도 한다[3].

즉 포스트 코로나 시대와 재택근무의 보편화에 대비하여 안전한 비대면 사회를 정착 및 유지하고, 더 나아가 국가경쟁력을 더 강화하기 위해서는 사이버보안체계의 수립이 필수적이며, 이를 위한 장기적이고 지속적인 연구가 필요하다[3].

2.2.2. 정보보호 환경 변화

2019년 12월을 시작으로 2020년은 코로나19 팬데믹으로 생활과 경제활동 전반이 변화되었다. 이로 인한 정보보호 환경도 전면적이며 일상적인 사이버 위협 대응체계로의 전환을 필요로 하고 있다[3].

이러한 영향으로 재택근무, 원격근무, 화상회의 등 비대면 서비스의 증가하였으며, 전통산업과 ICT 간 융합이 고도화, 가속화되면서 사이버 영역이 확장되고, 사이버 보안 위협 또한 전방위적으로 증가하고 있다.

코로나19 팬데믹 상황을 악용한 피싱 공격, 메일 사칭, 랜섬웨어 등의 사이버 공격과 사회공학적 기법을 이용한 공격이 급증하고, 단기간 급성장한 비대면 서비스에 대한 사이버 보안 위협과 비대면 서비스를 목표로 하는 사이버 보안 침해사례가 계속적으로 발생하고 있다.

비대면 서비스의 증가와 사이버공격이 점차 지능화됨에 따라 단말기와 원격망, 클라우드, 공급망 등 부문별 환경을 고려되어 체계화된 사이버방역체계가 요구된다[3].

2.3. 재택근무

2.3.1. 재택근무 정의

재택근무(在宅勤務, telecommuting, remote work)는 근로 형태의 일종으로, 정보 통신 기기 등을 활용하여 시간과 장소의 제약을 받지 않고 유연하게 일할 수 있는 형태를 말한다[4].

2.3.2. 재택근무 현황 및 전망

2019년 12월 코로나19 바이러스 감염병이 전 세계적인 유행으로 근로자의 안전을 위해 전 세계 다수 기업에서는 재택근무 제도를 도입하고 있다.

2020년 04월 소프트웨어정책연구소에서 발표한 보고서에 따르면 코로나19 바이러스 감염병 발생 이전인 2017년 08월 기준으로 국내에서 유연 근무를 활용하는 기업은 11%, 이 중 재택 및 원격 근무제도 활용 비

중은 5.8%에 불과했지만, 코로나19 바이러스 감염병 발생 직후 재택근무를 체험한 경우는 36%로 증가했다[5]. 이후 이를 계기로 크게 확대된 재택근무 실시 현황에 대해 2020년 07월 고용노동부는 잡플래닛에 위탁하여 5인 이상 사업장의 인사담당자 400명과 근로자 878명을 대상으로 조사를 실시하였다[6].

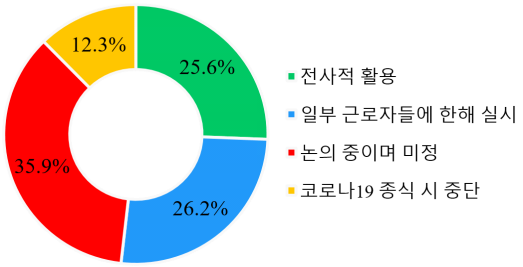
기업 인사담당자 조사 결과, 아래 [표 1]와 같이 재택근무를 운영한다는 응답이 48.8%로 확인 되었으며, 기업 10곳 중 5곳은 재택근무를 이미 도입한 것으로 나타났다[6].

위 두 조사에 따르면 코로나19 바이러스 발생 이후 많은 기업들이 재택근무제를 도입하였고, 그 비중이 점차 증가하는 것으로 나타났다.

〔표 1〕 기업 유형별 재택근무 운영 여부〔6〕

구분	전체 (단위: %, 개소)	기업유형			
		중소,중견기업	대기업	공공기관	기타
운영	48.8% (195)	47.8% (170)	58.3% (21)	50.0% (1)	50.0% (3)
미운영	51.2% (205)	52.2% (186)	41.7% (15)	50.0% (1)	50.0% (3)
전체	100% (400)	100% (356)	100% (36)	100% (2)	100% (6)

재택근무 운영으로 감염병 위기 대처 능력과 근로자 직무만족도 등 업무효율성로 긍정적인 결과가 확인되고 있다. 코로나19 바이러스 종식 이후에도 재택근무를 일부 근로자에 한해 계속 시행한다는 응답이 51.8%로 절반 이상 높게 나타났다. 향후 상시적 근무방식으로 정착할 가능성이 높은 것으로 확인되었다.



〔그림 2〕 재택근무 지속 여부 조사결과〔6〕

[그림 2]처럼 향후 다수 기업에서는 재택근무제도를 점차 도입할 것으로 예상되며, 재택근무 시 주로 활용되는 가상사설망에 대한 이용도 같이 증가 될 것으로 예상한다.

가상사설망의 이용이 증가할수록 사이버보안 위협도 같이 증가 할 것이며, 보안관제에서도 대응할 수 있는 정보보호 정책과 체계가 필요하다.

2.4. 보안관제

2.4.1. 보안관제 정의

보안관제의 정의는 기업의 자산, 정보, 기술과 같은 IT 자원을 해킹, 바이러스 등의 사이버 공격으로부터 보호하기 위한 일련의 활동 및 감시활동을 의미한다[7].

보안관제의 주업무는 해킹 사실을 기관에 통보하고 분석 단계에서 파악된 공격자 정보와 취약점 정보를 활용하여 피해 시스템이 정상적으로 운영될 수 있도록 신속하게 전문기술을 제공하는 것이다[8].

2.4.2. 보안관제 무중단의 원칙

보안관제에서의 무중단의 원칙은 사이버 공격을 신속히 탐지, 차단 및 대응하기 위해서는 24시간 365일 실시간으로 중단없이 보안관제 업무를 수행해야한다[7].

이를 위해 보안관제센터 운영 기관 또는 민간 보안관제 서비스 업체는 적정 수의 보안관제 인력을 보유하여 24시간으로 운영하는 교대근무 체계를 구축하고 있다[7].

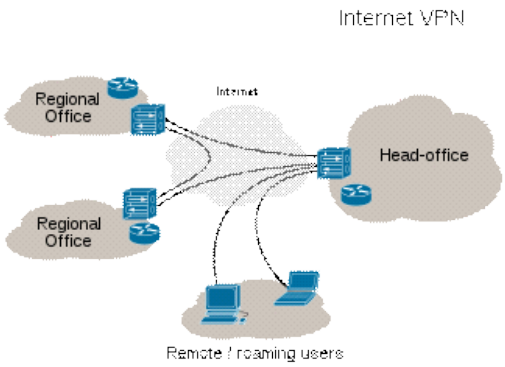
보안관제는 중단없이 상시적으로 사이버 공격에 대응해야 하기 때문에 이에 대응할 수 있는 서비스는 중단되지 않아야 한다.

2.5. 가상사설망(VPN, Virtual Private Network)

가상사설망(VPN)의 정의는 Virtual Private Network의 약자로 공중 네트워크를 통해 한 기업 및 몇몇 단체가 내용을 외부인에게 드러내지 않고 통신을 위한 목적으로 쓰이는 사설 통신망이다[9].

재택근무와 외부기업과의 정보전달을 위해 다수 기업에서는 VPN 장비를 도입하여 외부에서 가상사설망을 통해 트래픽을 유입하고 있다.

아래의 [그림 3]은 기업에서 운영하는 가상사설망의 일반적인 VPN 네트워크 구성도이다.



〔그림 3〕 VPN 연결 방식[9]

Ⅲ. 가상사설망 관련 프로토콜과 기술

3.1. VPN 터널링 프로토콜

VPN 터널링 기술은 두 종단(End-to-End) 사이에 가상의 통로를 형성하는 기술이다. 위 터널링을 지원하는 프로토콜을 VPN 터널링 프로토콜이라 한다[10].

네트워크 계층 별로 2계층의 터널링 프로토콜은 PPTP, L2F, L2TP가 있고, 3계층의 터널링 프로토콜은 IPSec, MPLS, GRE가 있다[10].

〔표 2〕 주요 VPN 터널링 프로토콜[10]

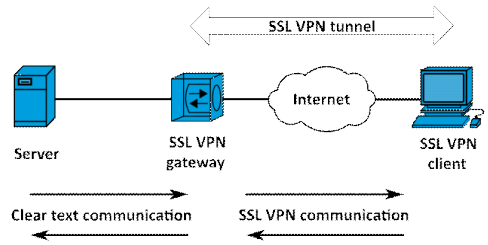
구분	PPTP	L2TP	IPSec
표준화	Microsoft	FRC 2661	RFC 2401
계층	2 계층	2 계층	3 계층
데이터 암호화	없음	없음	패킷 단위

3.2. 보안 소켓 계층(SSL, Secure Sockets Layer) 기반 가상사설망

보안 소켓 계층(SSL)은 프로토콜 기반으로 한 가상사설망 정보 처리 방법이다.

SSL은 웹 브라우저와 서버 간의 통신에서 정보를 암호화하는 SSL 보안 프로토콜을 사용하기 때문에, SSL-VPN 장비는 구축이 간편하고 비용이 적게 드는 장점이 있다.

반면 인터넷 프로토콜 보안 프로토콜을 이용하는 IPsec VPN 통신 방법은 별도의 하드웨어 장비가 필요하다[11].



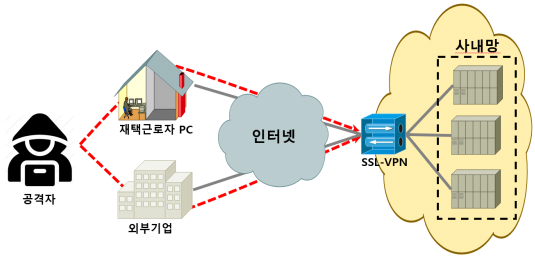
〔그림 4〕 SSL-VPN 통신과정[12]

Ⅳ. 가상사설망 사이버위협과 보안 강화 기술

4.1. 가상사설망 사이버 위협

가상사설망에서는 주로 재택근무자의 업무관련 정보 및 업무 상 필요한 외부기업의 정보가 전송되고 있다. 일반 근로자의 경우 정보보호관련 직무담당자보다 상대적으로 보안인식이 부족하다. 이로 인해 근로자의 부주의로 사이버 공격 대상의 주 목적이 될 수 있다. 특히 중소기업인 경우 정보보호 투자비용이 상대적으로 낮은 점을 고려하여 제3 공격자에 의해 악용될 수 있다. 일반적인 가상사설망 네트워크 구조는 최상단에 VPN 장비가 구성되어 있다.

아래의 [그림 5]와 같이 재택근무자 및 외부기업에서 전송된 통신은 VPN 장비를 통해 유입되며, 만약 재택근무자의 PC와 외부기업의 시스템을 악용하여 제3 공격자에 의해 경유지가 될 수 있다. 만약 사이버 공격 성공 시 기업자산정보 유출, 업무수행의 중단, 기업 이미지 악화, 금전적인 손해 등 큰 피해가 발생할 수 있다.



〔그림 5〕 가상사설망 사이버 공격 유입과정

4.1.1. 네트워크 스캐닝 공격 가능성

제3 공격자는 사이버 공격을 수행하기 위해 우선 스

캐닝 공격 시도를 하여 정보수집을 위해 대상 시스템의 취약한 서비스 포트를 확인을 한다.

한국원자력학회 춘계학술대회 참고문헌[10]에서 네트워크 스캐닝 공격 실험으로, VPN, Firewall 장비에 대해 포트 스캐닝을 한 결과, TCP를 사용하는 포트는 8888번만 열려져 있는 것으로 확인되었다. 하지만, 접근은 차단되어 접속은 불가능 된 것으로 확인되었다[10].

추가로 VPN, Firewall 장비의 내부 네트워크(Trusted)에서 VPN 장비에 대한 정보수집을 위해 “Nmap” 도구를 이용하여 포트 스캐닝을 수행하였다. 실험결과, VPN 장비 자체에서 패킷 접근 차단으로 공격은 실패하였다[13].

4.1.2. 서비스 거부 공격(DoS, Denial Of Service) 가능성

코로나19 바이러스 감염병과 같은 팬데믹 발생으로 재택근무가 급격히 증가하는 경우와 외부 공격자에 의해 서비스 거부 공격(DoS) 수행 시 많은 트래픽이 증가 할 것으로 예상한다.

트래픽 증가 시 가상사설망 내 VPN 장비 및 방화벽의 CPU 부하가 증가하여, 시스템의 기능을 제대로 수행하지 못할 가능성이 있다[13].

이러한 트래픽이 증가 할 경우 시스템의 가용성에 문제가 생길 가능성이 있다. 재택근무 수행에 있어서 시스템 복구 전까지 업무 상 큰 피해가 있을 것이며, 이에 대한 DDoS 장비를 도입하여 트래픽 임계치 설정이 필요하다.

4.1.3. APT(Advanced Persistent Threat) 공격 가능성

제3 공격자는 가상사설망 연결되는 점을 악용하여 APT 공격을 지속적으로 사이버공격을 수행 할 가능성이 있다. 기업 내에서 망분리로 인한 망 접점관리가 소홀할 경우 내부시스템에 악성코드가 전파 될 수 있기 때문에 그 보안위험은 매우 크다.

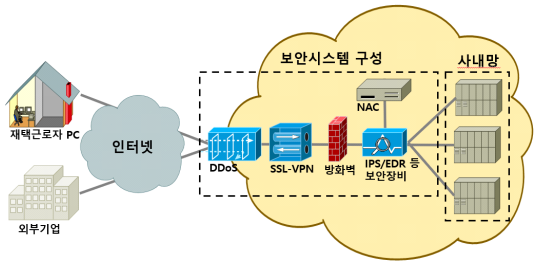
만약 재택근무자의 PC, 외부기업의 특정서버 등 사이버 공격을 수행 할 경유지로 사용되는 경우 내부시스템에 대한 많은 피해로 기업자산정보 유출, 기업이미지 악화, 금전적인 손해 등 큰 피해가 발생할 수 있다.

이를 예방하기 위해 기업 상황에 맞춰 사전 보안위협에 대응 할 수 있는 보안시스템이 추가적으로 필요하다.

4.2. 가상사설망 보안 강화 기술

아래 [그림 6]는 가상사설망으로 유입되는 사이버 위협으로부터 예방할 수 있는 가상사설망 보안시스템 구성 안이다. 기업의 상황과 여건에 따라 다양하지만 우선적으로 재택근로자의 업무 여건에 맞춰 DDoS 보안장비의 임계치 설정과 방화벽 보안장비의 최소 허용된 보안정책을 추가 설정한다.

추가로 구축 할 보안장비에 대해서는 기업 내 정보보호 담당자, 보안관제 담당자, 네트워크 담당자, 사내 IDC(Internet Data Center) 담당자 등 해당 분야 관련 담당자와 협의 하에 최선의 가상사설망 구성을 의논하여 구축하는 것을 권장한다.



〔그림 6〕 가상사설망 보안 네트워크 구성(안)

4.2.1. DDoS 보안장비 운영

가상사설망에서의 과다 트래픽이 발생될 것이 예상되는 상황일 경우 사전에 트래픽 허용치와 이벤트를 조정한다. 만약 비정상적으로 임계치가 증가하거나 공격 트래픽이 발생하는 경우 Drop시킨다.

재택근무가 증가할 상황인 경우 업무 간 필요한 이벤트 탐지 및 차단 설정과 임계치를 평소 대비 높게 설정하여 업무 관련 사내시스템에 영향이 없도록 한다.

감염병 유행으로 정부에서 사회적 거리 두기 제도를 시행되는 경우 단계별로 재택근무를 실시해야한다. 특히 사회적 거리 두기 3단계인 경우 기업에서는 필수인력 이외 재택근무를 의무화하기 때문에 급격히 트래픽 사용량이 증가 할 수 있다. 이러한 상황을 대비하여 기업 상황과 인력 수에 따라 사회적 거리 두기 단계별 재택근무 인원 기준으로 트래픽 임계치에 대한 조정 방안을 마련하는 것을 권장한다.

4.2.2. 방화벽(Firewall) 보안장비 운영

가상사설망에서의 방화벽은 사전에 공유된 재택근무자의 IP, 업무상 필요한 대상 시스템 IP, Port에 대해서만 양방향 허용 정책을 추가한다.

악성행위가 공유된 IP와 사전에 공유되지 않은 IP를 모두 차단 정책으로 추가한다. 차단 정책을 추가하게 되면 재택근무 및 사내시스템 외부 유출·유입되는 트래픽에 대해 예방조치가 될 뿐만 아니라 차단로그를 활용한 행위분석을 할 수 있다.

보안관제 수행 시에는 허용된 로그 중에서 사전에 공유되지 않은 IP에 대해 모니터링을 수행하면 된다. 공유되지 않은 IP가 탐지된 경우 로그 분석을 해야한다. 로그 분석 결과를 바탕으로 방화벽 보안장비에 맞는 정책과 설정을 적용해서 보안을 강화해야한다.

이러한 방화벽 보안정책으로 재택근무자와 업무상 필요한 대상 시스템과 1 대 1 단일 통신으로 전달되어 외부트래픽에 대한 영향이 없어 안전하다.

4.2.3. NAC(Network Access Control) 보안장비 운영

재택근무 시 근로자의 업무용 PC로 업무를 수행하여 단말기에서의 보안은 매우 중요하다.

아래 [표 3]과 같이 NAC의 주요 기능인 접근 제어/인증 외 다수 기능 등 활용하여 PC 보안안전 상태 점검 및 최소한의 정책 조건으로 통제를 해야한다.

〔표 3〕 NAC 주요 기능〔14〕

분류	주요기능
접근 제어/인증	• 내부 임직원 역할 기반의 접근 제어 • 네트워크의 모든 IP 기반 장치 접근 제어
PC 및 네트워크 장치 통제(무결성 체크)	• 백신 관리 • 패치 관리 • 자산 관리 (비인가 시스템 검출)
해킹, 웜, 유해 트래픽 탐지 및 차단	• 유해 트래픽 탐지 및 차단 • 해킹 행위 차단 • 증거 수집 능력

NAC의 주요기능을 활용한 운영방식은 다음과 같다.

접근제어/인증의 기능은 근로자의 업무용 PC에 NAC Agent를 설치하여 사전에 정보보호 담당자에게 공유된 IP 및 사용자 정보를 바탕으로 인증하여 운영을 권장한다.

PC 및 네트워크 장치 통제(무결성 체크)는 기업 내 정보보호정책에 따라 재택근무 시 외부 인터넷을 차단하고 업무와 관련된 사내시스템과 1 대 1 단일 통신을 하도록 해야한다. 또한, 보안위험이 있는 소프트웨어 설치여부 점검과 필수 보안소프트웨어 설치 및 최신버전이 확인 등 최소한의 PC 보안안전 상태를 점검하여 통제해야한다.

아래 [표 4]는 금융보안원에서 발간 한 “금융회사 재택근무 보안 안내서” 자료에서 내부망 접근통제에 대한 내용이다. 업무상 최소한의 IP 및 PORT로만 연결 허용, 미인가 IP 접속 차단 등의 보안조치를 의무적용되어야 한다[15].

〔표 4〕 금융회사 내부망 접근통제〔15〕

구분	세부내용	비고
최소한의 IP 및 Port로만 연결 허용	외부 단말기가 업무상 필요한 내부 시스템에만 접속할 수 있도록 접속 가능한 IP 및 Port를 통제	의무사항
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	권고사항

이처럼 재택근무 시 업무용 PC가 외부 인터넷과 연결되어 보안위협에 많이 노출되는 만큼 업무용 PC 단말기에 대해 엄격한 보안관리는 필수이다.

4.2.4. 상황별 보안 장비 추가 강화 운영

기업상황과 여건에 따라 도입되는 보안장비는 매우 다양하다. 제 3 공격자에 의해 유입되는 사이버 공격과 재택근무자의 부주의로 인한 PC 악성코드 감염 등 고려하면 더욱 많은 보안장비를 구축을 하여 보안관제를 수행 해야 한다.

재택근로자 PC에 대한 위협이 높은 만큼 우선적으로 호스트기반의 침입탐지시스템(HIPS)와 엔드포인트 위협탐지 및 대응 시스템(EDR)과 같은 호스트 기반의 보안장비 및 악성코드를 탐지할 수 있는 보안장비 등 구축하여 기업 상황과 여건에 맞는 보안관제를 권장한다.

하지만 중소기업에서는 가상사설망, 보안장비를 추가 구축하는데 높은 비용 투자와 보안서비스를 운영하는데 어려운 점이 있다.

4.3. 가상사설망 보안관제 인력

재택근무는 주로 평일 주간 근무 간 업무 수행하는 경우가 많아 평일 주간 근무에 집중 모니터링이 필요하다. 하지만 다른 분야의 보안관제와 병행하여 업무를 수행한다면 평일 주간근무 시간대 보안관제요원은 업무 과다에 대한 부담으로 실효성이 있는 대응이 불가능 할 수 있다.

이를 위해 별도 가상사설망을 관리할 수 있는 보안담당자 및 주간 전담 보안관제요원을 지정해야한다. 기존에 운영되었던 보안관제와 공동 대응으로 평일 주간 근무 위주로 대응을 하는 것이 효율적이다. 평일 주간 근무 외 대응은 비교적 여유로운 기존에 운영하고 있는 보안관제에서 대응을 수행한다.

4.4. VPN 관련 IP 주소 정보 등록

한국인터넷진흥원에 VPN 관련 IP 주소 등록을 하는 경우 사용하는 IP 주소가 실제 IP 주소가 아닌 VPN 서비스에 사용되는 IP가 변경 되었다는 사실을 알 수 있다[16]. 이러한 방법을 통해 등록된 IP 정보를 확인이 가능하다면 방화벽 정책 설정 및 보안장비 탐지 룰 설정을 통해 보안관제를 수행하여 사이버 보안 위협에 사전예방이 가능하다.

아래 [그림 6]과 같이 한국인터넷진흥원에서 IP조회가 가능한 서비스인 'WHOIS'를 이용하여 IP 정보와 사용목적에 대해 확인을 할 수 있다[17].

〔그림 7〕 한국인터넷진흥원 WHOIS IP조회 사이트〔17〕

V. 결 론

코로나19 바이러스 팬데믹으로 인해 재택근무의 수요가 증가함에 따라 가상사설망을 통한 재택근무의 수행률이 증가하였고 주로 이용되는 가상사설망의 보안에 대해서도 매우 중요해졌다. 현재 가설사설망을 대상으로 한 사이버 공격 시도가 증가함에 따라 보안관제를 활용한 보안 강화가 필요하다.

가상사설망에 대한 사이버 보안 위협에 대한 예방과 보안관제 대응도 매우 중요하지만, 이보다 더 중요한 것은 재택근무자의 보안 수칙을 지켜며 업무 수행 하는 것이다. 다수 기업에서는 이번 재택근무의 경험을 바탕으로 코로나19 바이러스 감염병 종식 후에도 재택근무제도를 계속 유지할 계획이다. 이는 앞으로 미래의 재택근무제도가 활성화 되고 보편화 됨에 따라 IT기술도 같이 고도화 될 것이고 보안의 중요성은 매우 크다.

향후, 미래의 안전한 보안을 위한 재택근무 제도에 대한 연구와 가상사설망에 대해 효율적인 사이버보안 위협 대응체계를 강화하는 것이 중요하다.

참 고 문 헌

[1] IT DALIY, "*[코로나19와 IT업계②] 이슈 악용한 사이버 공격 성행…원격·재택근무 확대에 보안 우려도*", http://www.itdaily.kr/news/articleView.html?idxno=100542, April 2020.

[2] 한국인터넷진흥원, "*사이버 위협 동향보고서(2020년 2분기)*", KISA 인터넷 보호나라&KrCERT, pp.36-41, July 2020.

[3] 국가정보원, "*2021 국가정보보호백서*", pp. 1-284, May 2021.

[4] 위키백과, "*재택근무*", https://ko.wikipedia.org/wiki/%EC%9E%AC%ED%83%9D%EA%B7%BC%EB%AC%B4, February 2021.

[5] 이명호, "*재택/원격근무와 미래의 일, 공간*", 소프트웨어정책연구소 월간SW중심사회 2020년 4월호, April 2020.

[6] 고용노동부 고용문화개선정책과, "*재택근무 업무 효율과 직무만족 모두 높게 나타나*", *고용노동부 보도자료*, http://www.moel.go.kr/news/enews/report/enewsView.do?news_seq=11450, September 2020.

[7] ADT캡스인포섹 공식블로그, "*'보안관제'에 관한 모든 것*", https://blog.naver.com/skinfosec2000/221116097157, October, 2017.
[8] 안성진, 이경호, 박원형. "*보안관제학*", 이한미디어, pp. 17, April 2014.
[9] 위키백과, "*가상사설망*", https://ko.wikipedia.org/wiki/%EA%B0%80%EC%83%81%EC%82%AC%EC%84%A4%EB%A7%9D, November 2020.
[10] 네이버블로그, "*VPN , 터널링프로토콜, IPsec*" https://blog.naver.com/daimon123/220426007711, July 2015.
[11] 한국정보통신기술협회 정보통신용어사전, *SSL 기반 가상 사설망, -基盤假想私設網, Secure Sockets Layer Virtual Private Network, SSL VPN*, http://word.tta.or.kr/dictionary/dictionaryView.do?word_seq=055060-3
[12] Michel Bakni, "*SSL VPN Topology-en.svg*", WIKIMEDIA COMMONS, https://commons.wikimedia.org/wiki/File:SSL_VPN_Topology-en.svg, November 2019.
[13] 김정수, 김종수, 박일진, 민경식, 최영명, 조도근, "*원격감시시스템에 가상사설통신망 적용을 위한 모의 해킹 시험*", 한국원자력학회 춘계학술발표회 논문집, 제7분과 : 방사선방어, pp.11-14, April 2003
[14] 양대일, "*정보 보안 개론 : 한 권으로 배우는 보안 이론의 모든 것*", 이한미디어, pp. 452, June 2013.
[15] 금융보안원, "*금융회사 재택근무 보안 안내서*", https://www.fsec.or.kr/user/bbs/fsec/147/315/bbsDataView/1549.do?page=1, 금융보안원 자료마당 가이드, November 2020.
[16] 이준기, 박광선, "*가상사설망을 이용한 사이버범죄의 대응 방법*", 한국디지털포렌식학회 디지털포렌식 연구 7권 1호, pp. 71, December 2013.
[17] 한국인터넷진흥원, "WHOIS", https://후이즈검색.한국/, 2016.

〈저자소개〉

강 동 윤 (Dongyoon, Kang)
2020년 2월 : 극동대학교 산업보안학과 공학사 졸업
2020년 9월~현재 : 동국대학교 국제정보보호대학원 정보보호학과 석사과정
<관심분야> 모의해킹, AI보안, 클라우드보안

이 상 웅 (Sangwoong, Lee)
2017년 2월 : 극동대학교 산업보안학과 졸업
2021년 3월~현재 : 동국대학교 국제정보보호대학원 사이버포렌식학과 석사과정
<관심분야> 정보보호, 디지털포렌식, 네트워크보안

이 재 우 (Jeawoo, Lee)
美 University of Southern California, Major : System Management 석사 졸업
건국대학교 정보체계학과 박사 졸업
한국정보보호진흥원 초대원장(전)
한국정보시스템감사통제협회 2대 회장(전)
한국CISSP협회 초대회장(전)
한국사이버포렌식전문가협회 초대회장(전)
(ISC)² 아시아 지역 회장(현)
동국대학교 국제정보보호대학원 정보보호학과 석좌교수(현)
<관심분야> 정보보호, 융합보안, AI보안

이 용 준 (Yongjoon, Lee)
1999년 2월 : 강남대학교 전자계산학과 공학사
2001년 2월 : 숭실대학교 컴퓨터공학과 공학석사
2005년 2월 : 숭실대학교 컴퓨터공학과 공학박사
2020년 4월~현재 : 극동대학교 해킹보안학과 조교수
<관심분야> 클라우드, 보안관제, AI·사이버보안 융합기술