



Comparative Analysis of Security Solutions for Remote Work

So-Yeon Kim, Yeong-Min Ha and Sangyong Choi

EasyChair preprints are intended for rapid dissemination of research results and are integrated with the rest of EasyChair.

August 2, 2020

원격근무를 위한 보안 솔루션 비교 분석

Comparative analysis of security solutions for remote work

요 약

최근 코로나19의 확산으로 원격근무가 기업의 업무 표준으로 자리 잡고 있다. 원격근무는 출퇴근 시간의 단축뿐만 아니라 코로나와 같은 감염병이 확산될 때 비교적 안전하게 근무를 수행할 수 있는 편리한 방법이지만, 정보통신기술을 이용한 데이터의 전송, 내부 시스템 접속 등 환경에 따라 다양한 사이버보안 위협이 발생하고 있다. 따라서, 원격근무를 시행함에 있어 정보보안은 기업이 반드시 고려해야만 하는 키워드이며, 다양한 원격근무 환경에서 기업의 자산을 사이버 위협으로부터 보호하기 위한 방안이 필요하다. 하지만 기업 보안담당자 입장에서는 산재되어 있는 다양한 솔루션을 일일이 조사하여 근무환경에 가장 적합한 보안솔루션을 선택하는 것은 많은 어려움이 따른다. 따라서 본 연구에서는 기업 보안담당자에게 도움을 주고 안전한 원격근무 환경을 구축하기 위한 보안솔루션 선택의 편의성 제공을 목표로 한다. 목표 달성을 위해 원격근무의 특성에 따른 보안위협을 조사하고, 보안위협을 완화하기 위해 다양한 원격근무 보안솔루션들을 비교·분석하여 원격근무의 특성에 최적화된 보안 아키텍처를 제안한다.

ABSTRACT

With the recent spread of Covid-19, teleworking has become a business standard for enterprises. While teleworking is a relatively safe way to work when infectious diseases such as corona spread as well as shorter commuting hours, various cybersecurity threats are occurring depending on the environment, such as the transmission of data using information and communication technology and access to internal systems. Therefore, information security is a keyword that an entity must consider in implementing remote work, and measures are needed to protect its assets from cyber threats in various remote work environments. However, from the perspective of corporate security officers, it is difficult to select the most suitable security solution for the working environment by examining various scattered solutions one by one. Therefore, this study aims to provide the convenience of choosing a security solution to assist corporate security personnel and establish a secure remote working environment. To achieve the goal, we investigate security threats according to the characteristics of telework, compare and analyze various remote security solutions to mitigate security threats, and propose a security architecture optimized for the characteristics of telework.

Keywords: Covid-19, Remort Work , Security Solution

I. 서 론

최근 정보통신기술의 발전과 업무문화의 변화로 원격근무로의 근무형태를 전환하는 기업들이 늘어나고 있다. [1] 또한 코로나19 팬데믹의 영향으로 가속화되어 원격근무는 기업의 업무 표준으로 자리 잡고 있다. 원격근무는 안전하게 근무를 수행할 수 있는 편리한 방법이지만, 최신 정보통신기술을 이용함에 따라 다양한 사이버보안 위협도 존재한다. 따라서, 원격근무를 시행함에 있어 정보보안은 기업이 반드시 고려해야만 하는 키워드이다. 기업의 중요 자산을 위협으로부터 지키기 위해 원격근무환경에 적절한 보안 솔루션을 적용시켜야하지만 기업 보안담당자 입장에서는 근무환경에서 산재하는 위협을 정확히 파악하여 적절한 보안 체계를 구축하기 쉽지 않다. 본 연구에서는 보안담당자에게 도움을 주고 안전한 원격근무 환경을 구축하기 위해 원격근무환경에 따른 보안 솔루션들을 조사하고, 여러 분류 기준을 두어 비교 분석한다. 또한 위협, 보안기능을 이용한 정성적 분석 결과를 반영하여 원격근무환경에서의 보안 솔루션 아키텍처를 제안한다.

II. 관련 연구

2.1 원격근무의 정의

원격근무(teleworking 혹은 telecommuting) 개념은 1973년 미국 캘리포니아대학 비레연구센터의 Jack Nilles가 보험회사의 원격근무 시범프로젝트를 수행하면서 최초로 사용되었다. 개인용 컴퓨터 통신이나 팩스 따위를 활용하여 자택이나 휴양지 따위와 같이 사무실에서 떨어진 장소에서 업무를 수행하는 일이자 개인용 컴퓨터를 통신 회선을 통해 개인용 컴퓨터 통신 센터의 주 컴퓨터와 연결하여, 개인용 컴퓨터 통신 회선 상호 간에 메시지나 데이터를 교환하고, 호스트에 축적된 정보를 검색하거나 예약, 주문 따위의 정보 처리 서비스를 제공하는 것이다. [2]

하지만 원격 근무에 대한 정의는 정보통신기술의 발달과 응용으로 재택근무, 원격근무센터, 이동원격근무 등 다양한 형태로 변하고 있다.

2.2 원격근무의 유형

원격근무의 유형은 원격근무를 어떻게 정의하는가에 따라서 포괄하는 범주가 달라지지만 가장 일반적인 분류는 근무 장소를 기준으로 한다. [2]

Table 1. Type of remote work

Type	Description
Telecommuting	Types of workers working at home using information and communication technology
Remote Work Center	a remote office with a working environment far away from the main office
Mobile remote work	It is the type of work where people contact, provide information, and report anywhere, including trains, trains, airplanes, hotels, etc. while moving places using offices, portable PCs, and mobile phones everywhere.

2.3 원격근무에 대한 위협

많은 기업이 코로나19 확산 방지를 위해 비대면 근무를 지원하는 협업 플랫폼으로 이전하고 있다. 이로 인해 새로운 보안 위협이 발생할 것으로 전망된다. 슬랙이 미국 증권거래소에 제출한 기업공개 문건에 따르면 기업용 커뮤니케이션 소프트웨어의 잠재적 보안 위협이 언급되고 있다. 특히 벨웨어, 바이러스, 랜섬웨어 등이 위협 요소로 지적됐다. 액센추어의 2019년도 사이버 범죄 관련 보고서는 피싱 및 소셜 엔지니어링 공격을 겪은 기업의 비율이 1년 만에 16% 상승한 83%를 기록했다고 밝혔다. 위와 관련하여 원격근무의 보안 위협을 아래와 같이 5가지로 분류하고 있다. [3][4][5]

- ① 엔드포인트 장비/단말에 대한 위협
- ② 사용자 계정 및 접근권한 관리
- ③ 취약한 네트워크를 통한 중요정보 전송
- ④ 재택근무 관련 원격접속 로그 기록 보관 위협
- ⑤ 웹캠 관련 해킹 및 애플리케이션 위협

원격근무의 보안위협은 앞서 제시한 다섯가지 뿐만 아니라 끊임없이 파생되어 산재한다. 이에 원격근무에 대한 보안위협을 위협 사례를 중심으로 [시스템/OS ,

Category	Threats
----------	---------

System / OS	Mac User Target Attack
	endpoint equipment, related devices
	weak access control
Network	Connection to an insecure network
	Vulnerabilities due to Multiple Remote Access Points
	Threats to Endpoint
Application	Use of vulnerable FTP, mail services
	Threats to Web , DNS
	Webcam-related hacking
Information Protection General	Remote Access Log Threat
	Phishing for employee accounts
	Critical Data Leakage

네트워크 , 애플리케이션 , 정보보호일반/사회공학]의 4가지 카테고리로 분류기준을 삼아 Tables 2와 같이 분류하였다.

2.4 위협에 대한 보안기능

앞서 살펴보았듯 원격근무에 대한 많은 위협들이 산재하고 있다. 그에 대처하기 위해 많은 기업들과 기관들이 원격근무에 대한 정보보호 실천 수칙 또는 가이드를 내놓고 있다. 해당 보안 가이드와 정보통신보안의 이론적인 부분, 현업의 근무자의 증언을 통해 원격 근무 시 위협을 대처할 수 있는 보안 기능을 조사 Table 3. Security function against threat

Category	Security function
System / OS	Ability to maintain, support, and monitor system security levels of working PCs
	Deliver cloud services
	antivirus function
Network	Remote Access Point Restriction Feature
	User Authentication and Access Control
	Threat detection ,response capabilities
Application	Web Attack Detection
	filtering spam mail
	Ability to block threats to webcams, microphones, etc.
Information Protection General	Monitoring and logging features for remote access
	Critical Data Control Management
	mobile media blocking function

하였다. 보안 위협과 마찬가지로 4가지 카테고리로 분류해보았고 그에 대한 보안 기능을 정리하였다.[6][7]

III. 원격근무 보안 솔루션 분석

3.1 원격근무 보안 솔루션

본 연구를 위해 한국소프트웨어산업협회에서 제공하는 원격근무 솔루션 156건을 대상으로 하여 제안한 분류 기준을 통해 구조화하는 방법으로 연구를 진행하였다.[8] 또한, 최적의 보안 아키텍처 제안을 위해 원격근무의 특성과 정보보안 분야, 정보보안 분야별 위협, 위협에 대응하기 위한 보안기능, 보안기능을 지원하는 솔루션 간의 유기적인 매칭을 통해 구조화한다.

Table 4. Full Remote Work Security Solution

Solution	Description
WaterWall V 5.0	Manage internal information leakage in a cloud PC environment
런리모트	PC Remote Control Service.
다이렉트클라우드 그룹웨어	Delivers high reliability and essential groupware functionality
Microsoft Teams	Digital hub for collaboration with a wide variety of teams needed for work
시큐어디스크	Prevent document leakage and loss and provide a collaborative document security environment
무비업 스트리밍 솔루션/플랫폼	Provide secure videoconferencing
RemoteMV	PC Remote Control Service.
mcloudoc	Carry-out process, ransomware protection, seamless collaboration
vCloudPC	Secure virtual desktop delivery
Dstation	Solutions that provide user-specific virtual desktops and data storage
엠오피스	PC-OFF automation solution that controls PC usage time
MoBiCa(기업용 모바일 단말관리 솔루션)	Integrated terminal management, system access management, and information leakage prevention provided
Fasoo DRM	Data Security Solutions
Office Keeper	Integrated PC security-enabled information leakage prevention solution

LX UTM	integratedthreat management
트로이캣	An endpoint security solution that analyzes all processes and preemptively blocks malicious behavior.
VForce UTM	integratedthreat management
Office Messenger	E-Messenger with format and security
Nexoffice Meeting	Video conferencing solutions that enable meetings on a variety of devices and environments
Bizbox Alpha	Realize smart work through real-time communication and collaboration in a cloud-based mobile work environment
RemoteCall	PC Remote Control Service.

3.2 보안 솔루션 분류 기준 정립

전수조사된 원격근무 솔루션들을 분류하기 위해 분류기준을 정립하고자 한다.

먼저 일반적이고 범용적인 기준을 통해 간단히 분류를 하고, 부가적으로 솔루션에 대한 정보를 제공하고자 하는 대상이 솔루션을 어떤 목적으로 쓰는지, 어떤 근무환경을 가지고 있는지, 어떤 기업 규모/인원/자산을 가지고 있는지에 따라 분류 기준을 생성해 분류한다.

Table 5. Classification by Security Category

Category	Description
System / OS	Maintain security level for work terminals , solutions that control user authentication access in the system
Network	A solution that ensures secure networking for work-in-house network access and can be managed for remote access
Application	Solutions that can drive secure application use and defend against web attacks
Information Protection General	A solution that maintains a worker's internal network access records and provides strong control over critical documents.

정보보안에 관련된 4가지 카테고리 [시스템/OS , 네트워크 , 애플리케이션 , 정보보호일반/사회공학]으

로 분류 기준을 생성하였다.

Table 6. Classification by purpose of use

Purpose	Description
Communication Service / Remote Control	Solutions that provide safe communication services and control work terminals
Integrated data management	Solutions for easy centralized data management or leakage prevention of critical data
Groupware/ cooperative tools	Solutions that help employees collaborate while maintaining security or provide video conferencing, instant messaging, etc.
Delivering a Cloud Environment	A solution that provides cloud services to provide an environment for working.

원격근무 솔루션을 사용함에 있어 다양한 목적이 존재하는데, 대표적인 4가지 목적 [통신서비스/원격제어, 통합데이터관리, 그룹웨어/협업, 클라우드환경 제공] 으로 분류 기준을 생성하였다.

Table 7. Classification by corporate scale

Scale	Description
Large / Midsize Business	1000+++ , solution for a company with basic needs and sufficient assets
Small businesses	Solutions for companies with a small number of people and no organized working environment

원격근무를 시행하려는 기업의 규모/인원/자산에 따라 [대/중견기업 , 소규모 기업] 으로 분류 기준을 생성하였다.

3.3 보안 기능별 솔루션

Table 8과 같이 보안기능의 분류기준으로 하여 솔루션들을 매칭한 결과 System/os에 7종, Network에 3종, Application에 6종, InformationProtection General에 6종의 솔루션이 매칭되었다.

Table 8. Solutions by Security Function

System / OS	Network
-------------	---------

<ul style="list-style-type: none"> - 엠피스 - 트로이캣 - A-sonic - VCloudPC - Dstation - 다이렉트클라우드 - 링크미마인 	<ul style="list-style-type: none"> - LX UTM - VForce UTM - 매니지드 보안
Application	Information Protection General
<ul style="list-style-type: none"> - 협업툴 콜라비 - Microsoft Teams - 무비업 솔루션 - MoBiCa - Office Messenger - Nexoffice Meeting 	<ul style="list-style-type: none"> - OZ e-Form - 더존 Bizbox Alpha - Fasoo DRM - Office Keeper - WaterWall V 5.0 - 시큐어디스크

3.4 사용 목적별 솔루션

Table 9과 같이 사용목적 분류기준으로 하여 솔루션들을 매칭한 결과 Communication Service / Remote Control 에 5종, Intergrated Data Management에 5종, Groupware/Cooperative에 5종, Delivering a Cloud Environment에 2종의 솔루션이

Table 9. Solutions by Usage

Communication Service / Remote Control	Integrated data management
<ul style="list-style-type: none"> - RemoteMV - A-sonic - Seetrol - RemoteCall - 런리모트 	<ul style="list-style-type: none"> - WaterWall V 5.0 - 시큐어디스크 - Dstation - Fasoo DRM - Office Keeper
Groupware/cooperative tools	Delivering a Cloud Environment
<ul style="list-style-type: none"> - Microsoft Teams - 협업툴 콜라비 - 무비업 솔루션 - mcloudoc - Office Messenger 	<ul style="list-style-type: none"> - vCloudPC - Dstation

매칭되었다.

3.5 기업규모/인원/자산 별 솔루션

Table 10. Solutions by Company Size / Personnel / Asset

Large / Midsize	Small businesses
-----------------	------------------

Business	
<ul style="list-style-type: none"> - Mattermost - WaterWall V 5.0 - TeamViewer - 시큐어디스크 - mcloudoc - 엠피스 - Office Keeper - LX UTM - 트로이캣 - VForce UTM 	<ul style="list-style-type: none"> - Microsoft Teams - 협업툴 콜라비 - RemoteMV - vCloudPC - Dstation - MoBiCa - Office Messenger - ezsign - A-sonic

Table 10과 같이 보안기능의 분류기준으로 하여 솔루션들을 매칭한 결과 Large/Midsize Business 에 10종, Small businesses 에 9종의 솔루션이 매칭되었다.

IV. 안전한 원격근무 구축 아키텍처

3.3에서 제안된 Table 3. 보안분야/보안기능별 솔루션은 기능에 대한 분류기준을 통해 단순히 보안 솔루션들을 나열한 결과물이다. 그리하여 보안위협, 보안기능, 보안솔루션의 세 요소의 연관성을 정확히 파악하기가 어렵다. 이를 개선하기 위해 요소의 각 항목을 개체화한 후 개체 간의 유기적인 매칭을 통해 보다 직관적인 통찰력을 제공하였다.

4.1. 위협 평가

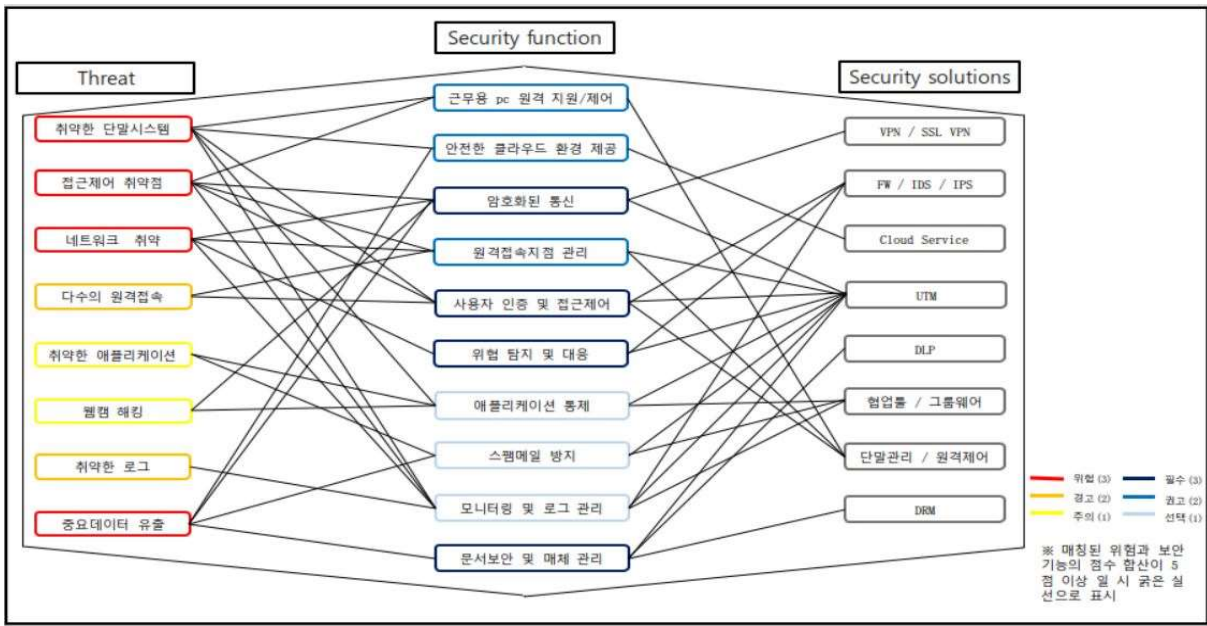
위협에 대한 각 요소는 위협 분석 평가 기준을 참고하여 위협(보호자산 손실로 인해 업무중단 등 심각한 영향을 초래), 경고(보호자산의 손실이 있으나, 업무에 심각하게 영향을 끼치지 않음), 주의(보호자산의 손실이 매우 경미함)으로 명시하였고 각각 3, 2, 1의 위험도 점수를 부여한다. [9]

4.2. 중요도에 따른 보안기능

보안기능에 대한 각 요소는 그 기능에 대한 중요도를 기준삼아 필수, 권고, 선택으로 명시하였고 각각 3, 2, 1의 기능중요도 점수를 부여한다.

4.3. 평가 및 매칭 방법

위협 평가를 통한 위협의 위험도, 기능적 중요도 평



가를 통한 기능중요도 등의 정성적 분석방법을 통해 각 요소들을 평가하였다. 하여 각 요소들간의 연관 관계가 형성된다면 실선을 통해 매칭될 수 있다. 또한 매칭된 위협과 보안기능의 점수 합산이 5점 이상 일 시 굵은 실선으로 매칭된다.

4.4. 분석 결과 및 활용 방안

Fig. 1과 같이 원격근무 환경에서의 위협, 보안기능, 솔루션 간의 아키텍처는 시스템과 사회공학 측면에서의 위협이 높은 위험도를 보여주며, 네트워크로 조직 내부와 연결함에 따라 네트워크 취약점이 높은 위협으로 분석되었다. 이를 보안하기 위해 ‘접근통제’, ‘보안 네트워크’를 지원하는 보안기능의 중요도가 높게 측정되었다. 결과적으로 해당 보안기능을 지원하는 ‘UTM’ 솔루션이 다수 매칭되었다. 이러한 분석 결과는 다양한 위협에 대해 우선순위를 결정하고 원격근무 환경을 구축하고자 하는 조직에서 비용 투자의 우선순위를 결정할 때 도움을 줄 수 있다.

V. 결론 및 한계점

5.1 연구의 한계점

본 연구에 있어 한계점이 존재하는데, 솔루션들의 분류기준은 그저 정보보안 이론과 사례화된 위협들을

바탕으로 생성하였기에 객관성이 부족하고 기준선 또한 모호할 수 있다는 점이다. 또한 보안 솔루션 아키텍처를 생성하기 위한 분석방법 중에도 한계점은 존재한다. 위협요소와 보안기능요소에 점수를 부여하는 과정에서 정성적 방법으로 평가를 하였기에 점수 부여가 모호해질수있다는 점이 또 하나의 한계로 나타났다. 이에 본 연구에 이은 후속 연구에서는 앞서 언급한 모호한 부분을 보완하여야만 한다. 예를 들어 ‘안전한 원격근무를 위해 솔루션을 도입하니, 보안 위협에 대해서 기존 대비 80% 이상의 개선효과를 보였다’와 같은 수치적 사례를 통해 정량적분석을 행하고 각 분석방법간의 균형을 유지시켜 연구를 발전시켜야한다.[10]

5.2 결론

코로나 사태로 인해 업무 표준이 된 원격근무를 시행함에 있어 안전한 근무를 지향하기 위한 각 회사의 보안 담당자들의 요구사항을 충족시킬 수 있는 원격근무 보안 솔루션 아키텍처에 대해서 살펴보았다. 제시한 아키텍처를 설계할 때 추구한 주요 목표 중의 하나는 원격근무에 대한 위협이 어떤 것이 존재하는지, 그에 대한 보안기능이 어떤것이 있는지, 보안기능을 수행할 수 있는 솔루션이 어떤 것이 산재하는지에 대해 전체적인 흐름을 파악 할 수 있게 인사이트를 제공 받을 수 있도록 한 점이다.

이를 위하여 한국소프트웨어산업협회에서 제공하는

원격근무 솔루션 156건을 대상으로 하여 제안한 분류 기준을 통해 구조화하는 방법으로 연구를 진행하였다. 연구를 통해 분류기준을 생성하였고 분류를 통하여 [보안기능별, 사용목적별, 기업규모별] 에 해당하는 솔루션 분류모델을 3종 생성하였다. 나아가 보안기능별 솔루션 모델의 한계점을 개선하기위해 정성적 분석방법을 이용한 [안전한 원격근무 구축 아키텍처]를 최종 연구결과물로 도출하였다.

결론적으로 솔루션의 이러한 원격근무 보안 솔루션 아키텍처를 성공적으로 개발하여 국내 업계 및 학계의 보안 담당자들에게 널리 보급하고, 이를 기반으로 원격근무 환경을 구축할 때, 사이버 보안 신뢰도를 확보할 수 있는 안전성이 보증되는 근무환경을 구축할 수 있을 것으로 기대한다.

References

- [1] Remort Work Trends, <https://www.criteo.com/kr/insights/%EC%BD%94%EB%A1%9C%EB%82%98-%EB%B0%94%EC%9D%B4%EB%9F%AC%EC%8A%A4-%EC%9B%90%EA%B2%A9-%EC%9E%91%EC%97%85-%EB%8F%99%ED%96%A5/>
- [2] Recommended Guide to Information ProtectionforSmartWorkActivationKISA , pp. 40-107, December 2011.
- [3] Remort Work Threat, <https://blog.alyac.co.kr/2852>
- [4] Remort Work Threat, <https://www.sisaweek.com/news/articleView.html?idxno=132492>
- [5] Remort Work Threat, http://m.ddaily.co.kr/m/m_article/?no=193261
- [6] Information Protection Rules for Home/Remote Work Environment, <https://blog.alyac.co.kr/2852>
- [7] Information Protection Rules for Home/Remote Work Environment and Six-Step Security ,

- <https://byline.network/2020/03/30-84/>
- [8] Remort Work, Education Solution, <https://www.sw.or.kr/site/sw/rs/rsList.do?solutionType=A>
- [9] ISMS-P risk assessment criteria, <https://blogger.pe.kr/792>
- [10] difference between qualitative and quantitative analysis, <https://infuture.kr/426>