Rationalization of Network Segregation for Continuity of Financial Services Following COVID-19

Manyong Choi[1], Jin Kwak[2]
[1] Dept. Computer Engineering, Ajou University
Gyeonggi-do, Korea
[e-mail: mychoi92@ajou.ac.kr]
[2] Dept. Cyber Security, Ajou University
Gyeonggi-do, Korea
[e-mail: security@ajou.ac.kr]
*Corresponding author : Jin Kwak

Received March 31, 2021; revised August 4, 2021; accepted Septebmer 21, 2021; published November 30, 2021

Abstract

As measures for protecting users and ensuring security of electronic financial transactions, such as online banking, financial institutions in South Korea have implemented network segregation policies. However, a revision of such domain-centered standardized network segregation policies has been increasingly requested because of: 1) increased demand for remote work due to changes resulting from COVID-19 pandemic; and 2) the difficulty of applying new technologies of fintech companies based on information and communications technologies (ICTs) such as cloud services. Therefore, in this study, problems of the remote work environment arising from the network segregation policy currently applied to the financial sector in South Korea and those from the application of new ICTs such as fintech technology have been investigated. In addition, internal network protection policies of foreign financial sectors, such as those of the United States, United Kingdom, European Union, and Russia, and internal network protection policies of non-financial sectors, such as control systems, have been analyzed. As measures for the effective improvement of the current network segregation policy, we propose a policy change from domain-based to data-centric network segregation. Furthermore, to resolve threats of hacking at remote work, recently emerging as a global problem due to COVID-19 pandemic, a standard model for remote work system development applicable to financial companies and a reinforced terminal security model are presented, and an alternative control method applicable when network segregation is not applied is proposed.

Keywords: COVID-19, Financial Service, Information Security, Network Segregation, Remote work

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. 2021R1A2C2011391).

http://doi.org/10.3837/tiis.2021.11.016 **ISSN : 1976-7277**

1. Introduction

As measures for protecting users and ensuring security of electronic financial transactions, such as online banking, South Korea has legally implemented a network segregation policy, which “separates, blocks, and prohibits access to external networks including internet from internal business systems connected to the internal network,” as stipulated in the Regulation on Supervision of Electronic Financial Businesses. Network segregation refers to “separating the information and communications technology (ICT) lines of financial companies into internal networks for business and external networks (internet) to prevent cyber threats and information leakage,” which has been introduced as a follow-up measure to the 2013 financial company computer network hacking incident. Network segregation is categorized into 'physical network segregation' using two personal computers (PCs), one for the internal business network and the other for internet, and 'logical network segregation,' with differentiated use of one PC in each network, depending on the composition of the structure [1]. The Regulation on Supervision of Electronic Financial Businesses specifies as targets for implementing network segregation the internal business system, information processing system located in the information technology (IT) room, and terminals directly connected to the system, as follows.

- Separating, blocking, and prohibiting access to external networks such as internet (including wireless networks) from internal business systems connected to the internal network (Article 15, 1–3);
- Information processing system located in the IT room and terminals that have a direct access to the system for operation, development, and security of the information processing system must be physically separated from external networks such as the internet (Article 15, 1–5).

Such standardized network segregation policy poses restrictions to the introduction of internet-based ICTs (fintech, cloud, etc.) and to financial companies planning to adopt state-of-the-art technologies based on the internet. Thus, improvement measures are required to address these limitations, which are perceived as excessive financial regulation. In addition, as working from home/remote work became inevitable for financial companies due to COVID-19, the Financial Supervisory Service (FSS) established the grounds for exceptions to network segregation as an emergency measure, allowing remote access. Accordingly, financial companies have quickly introduced working from home/remote work systems, but preparatory actions, risk assessment, and security measures for such systems have been insufficient.

In addition, current network segregation regulations implement network segregation in a standardized, undifferentiated manner without considering the business characteristics. Terminals of IT staff who are engaged in development, operation, and security of information processing systems that require seamless connectivity to external network should also apply physical network segregation. Thus, the IT staff productivity is reduced. As a result, there have been increasing requests for exceptions to network segregation. Therefore, it is necessary to diagnose the risk level in case of application of network segregation and respective exceptions according to the type of work and the importance of the data used. According to the assessed risk level, differentiated implementation of regulations is required to allow exceptions to physical network segregation for works that require external network access.

Physical network segregation is not mandatory to cloud services requiring network segregation exceptions, but the regulation stipulates that logical network segregation or alternative control measures, such as administrator rights removal of PC users and encrypted storage of terminal IT data (e.g., digital rights management), should be implemented. However, due to the procedures of cloud service providers, it is difficult to apply the alternative control measures specified in the regulation and the items are limited. Thus, although other technologies are available to replace network segregation, the application of alternative measures is still limited. Therefore, to implement a network segregation regulation that can be applied in practice considering the procedures of cloud service providers, alternative control measures should be specified or allowed in a provision within the regulation.

In addition, the application of network segregation exceptions is limited even when connection to external organizations is required for business, and it is applied without considering the nature of work and data. Furthermore, there are cases of inadequate management practices, such as frequently deleting data that has been exported to external organizations through an external network. As a result, the system becomes more vulnerable to information leakage. Therefore, it is necessary to allow self-determination of the scope of work applicable to network segregation exceptions through assessment of risk levels for secure connection with external organizations.

The number of people working from home/remote work increased in the financial sector since the COVID-19 outbreak. In particular, in March 2020, it almost doubled compared to the previous month due to the COVID-19 pandemic.

As the demand for telecommuting increases due to changes resulting from COVID-19 pandemic, there is a limitation in business continuity because of network segregation regulations. To provide the continuity of financial IT technology and services, studies on the rationalization of network segregation regulations are required. To this end, this study diagnoses the risk level aiming to establish criteria for implementation and exceptions for network segregation, analyzes the internal network protection technology that can replace network segregation, and compares and diagnoses the security level to derive various protection measures as alternatives to network segregation suitable for the work environment. In addition, based on the analysis, we propose an alternative method when network segregation is not applied in the financial sector, and a rationalization method of network segregation based on remote system configuration when working from home under the implementation of network segregation regulations.

This study is organized as follows. Chapter 2 describes the analysis of the problems of network segregation implementation in the domestic financial sector. Chapter 3 describes the regulations and cases of application for internal network security technology in overseas financial sectors and also analyzes the internal network security technology applied in domestic non-financial sectors. In Chapter 4, we propose a rationalization method for network segregation regulation based on the analyses in Chapters 2 and 3. Finally, Chapter 5 provides the conclusion of this paper.

2. Diagnosis of problems from network segregation in the domestic financial sector

This chapter describes the diagnosis of problems of the network segregation policy adopted in the domestic financial sector.

2.1 Problems of applying network segregation regulations when building a remote access system for working from home arrangement

Currently, there are five types of working from home systems classified by the FSS. The construction of remote access systems for working from home is possible for all types, but security controls must be observed for remote access.

2.1.1 VDI for remote access

The remote-access VDI is one of the available methods for working from home that do not have direct connections with ① external terminals and ④ work systems in the internal network. This is a system in which virtual desktop image is delivered through ③ VDI terminals in internal or external networks. Line encryption is performed using secure socket layer virtual private network (SSL VPN), IPSec VPN, and others, and authentication for remote access users is required. In addition, the ① external terminals for remote-access VDI should comply with protective measures, as follows:

- Installation of antivirus programs, real-time update, and test;
- Constant updates for the latest version of the operating system and programs used;
- Blocking of unauthorized software installation;
- Setting of login password and screen saver.

The remote-access VDI is highly secure and complies with the current network segregation regulations, but it is mainly applied and used by large financial corporations due to its high cost for system construction. Even if the terminal is attacked by a malicious code, the code cannot be introduced into the internal network, and data in the internal business network is not sent to the remote-access VDI terminal, thus preventing information leakage. Fig. 1 shows the composition of the system using remote-access VDI.

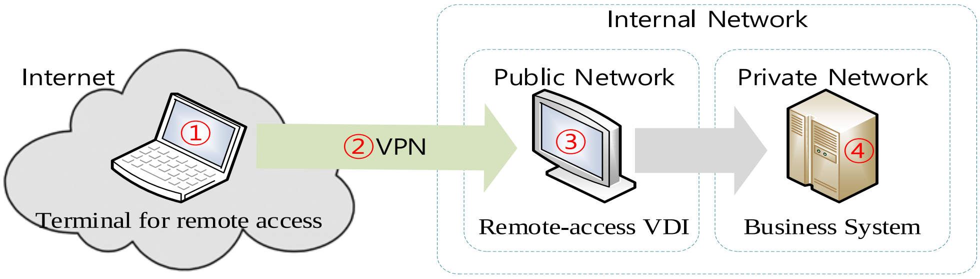


Fig. 1. Composition of the system using remote-access VDI

The model used in the financial sector with the introduction of remote-access VDI in Fig. 1 is the SSL VPN + in-house-built VDI model. The person working from home can run the SSL VPN program on the PC, log in with the given account, and access the virtual PC of the VDI server in the company’s internal system, which then allows the access to the work system.

As an example of a situation that can pose a security threat in the model shown in Fig. 1, information leakage can occur due to malware embedded in the PC used for working from home. When a remote administration tool is installed on the PC used for working from home or if the PC is infected with a malware that executes a man in the middle (MITM) attack, the account and password for working from home may be leaked [2,3]. In addition, a hacker may access VDI through a leaked account and infiltrate the internal network.

2.1.2 Cloud VDI

The cloud VDI is another method for working from home. It is not directly connected to the external ① terminals and ④ work system in the internal network, but the virtual desktop image is delivered through cloud VDI. Line encryption is performed using SSL VPN, and authentication for remote access users is required. In addition, the external terminals for ① remote-access VDI should comply with protective measures as follows.

- Installation of antivirus programs, real-time update, and test;
- Constant updates for the latest version of the operating system and programs used;
- Blocking of unauthorized software installation;
- Setting of login password and screen saver.

Similar to the remote-access VDI method, the cloud VDI has high security, low cost, and short period for construction. **Fig. 2** shows the system composition using the cloud VDI.

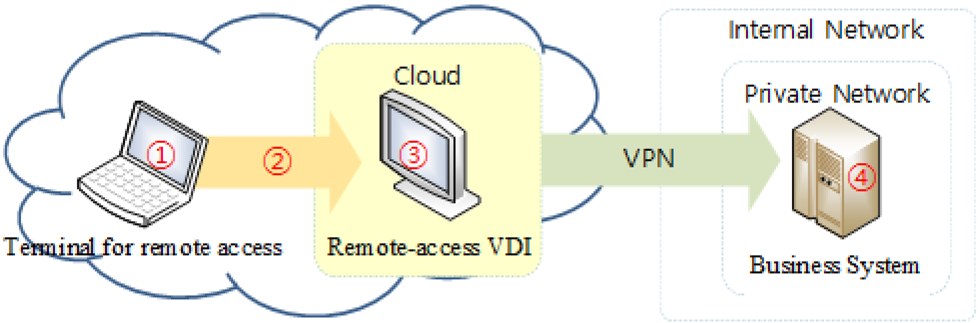


Fig. 2. Composition of the system using cloud.

The model actually employed in the financial sector using the method shown in **Fig. 2** is a composition of cloud VDI and SSL VPN. The person working from home can run the SSL VPN program on the PC, log in with the given account, and access the virtual PC of the VDI server in the cloud, which then enables the access to the work system

Cost is charged by time of use and quick installation is possible when needed, which resolves the issue of time and cost required for building a VDI server.

In the case of the system configuration shown in **Fig. 2**, security threats may arise due to inexperience in operating cloud services.

2.1.3 Direct connection using external access terminal

The method using an external terminal has limited availability and the access is made through an external ① terminal (owned either by the company or privately by the employee) directly to the ④ system in the internal network. Line encryption mainly uses SSL VPN and authentication for remote access users is required. In addition, the external ① remote-access VDI terminal must comply with the following protective measures:

- Installation of antivirus programs, real-time update, and test;
- Constant updates for the latest version of the operating system and programs used;
- Setting login password and screen saver;
- Blocking users from tampering with security settings;
- Blocking reading/writing of external storage devices such as USB;
- Blocking print-out;
- Blocking screen capture;

- Encrypted saving of IT data (e.g., files, documents);
- Disk encryption when using a laptop.

In the direct connection using an external terminal, the access is available to the remote access users with only a VPN account. Therefore, if a terminal with a high risk of malware infection is directly connected to the internal network, there is a high risk of malware transfer. ④ Work system information of the internal network can be stored in ① terminal, thus there is a high risk of information leakage. Connecting ① the terminal to the internet is a violation of the network segregation regulation.

Therefore, the system configuration using the external terminal can be used in limited cases when internet connection at the terminal is blocked, reinforced security is applied to the terminal, security control equivalent to exclusive use of the virtual private network is applied, or when a strictly managed authentication process is applied when accessing the system. **Fig. 3** shows the system configuration using an external terminal.

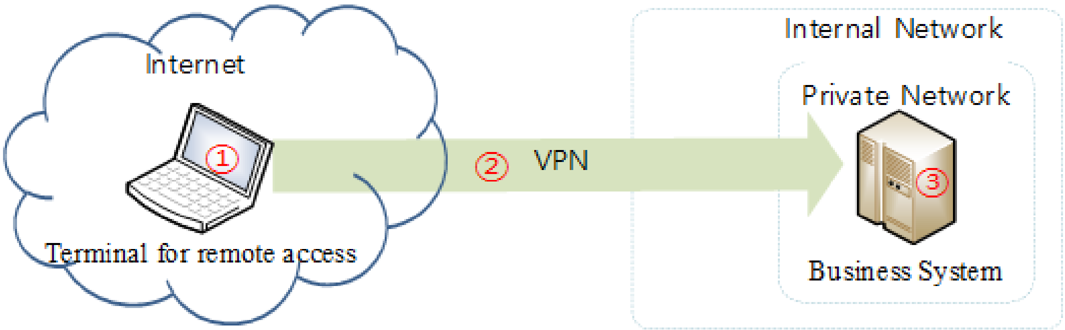


Fig. 3. Composition of the system using external terminals.

The model actually used in the financial sector applying the system configuration shown in **Fig. 3** is based on dedicated terminals and VPN.

In addition, remote workers can connect their smartphones (dedicated terminal) to the monitor and access the separately configured security Operating System area, execute the SSL program, and log in with the assigned account to access the work system.

In the system configurations shown in **Fig. 3**, the reliability of external terminals and programs is not guaranteed. To achieve the same security effect as using the external terminal in an internal network, technologies should be applied, such as limiting the use of the terminal for accessing the internal network and limiting the network that can be accessed. In addition, external terminals have vulnerabilities such as stealing personal information by exploiting weak points, including CVE-2019-10574 and CVE-2016-2431, to disable the tampering verification procedure for tampered applications [4].

2.1.4 PC remote access program

In this method, a remote access program is installed on the company's work terminal, which enables remote access from the ① terminal on the external network owned by the company or personally owned by the employee. Line encryption is performed using SSL VPN and authentication for remote access users is required. In addition, the external ① remote-access VDI terminals must comply with the following protective measures:

- Installation of antivirus programs, real-time update, and test;
- Constant updates for the latest version of the operating system and programs used;

- Setting of login password and screen saver;
- Blocking users from tampering with security settings;
- Blocking reading/writing of external storage devices such as USB;
- Blocking print-out;
- Blocking screen capture;
- Encrypted saving of IT data (e.g., files, documents);
- Disk encryption when using a laptop.

The PC remote access program can be used only by installing a remote program without any additional equipment, and does not require authentication, terminal security, and communication encryption for use. As this violates the FSS network segregation regulations, this method cannot be adopted as a system for remote work. **Fig. 4** shows the system configuration using the PC remote access program.

However, there are cases in which the financial sector uses this system configuration. For example, when a remote worker installs all remote access programs on terminals used at the company and at home, and log in to the remote access program when accessing the work system at home to access the work PC. In the financial sector, the authentication process has been tightened for security, and if a management system is built in the company, control of abnormal behaviors of users is also possible.

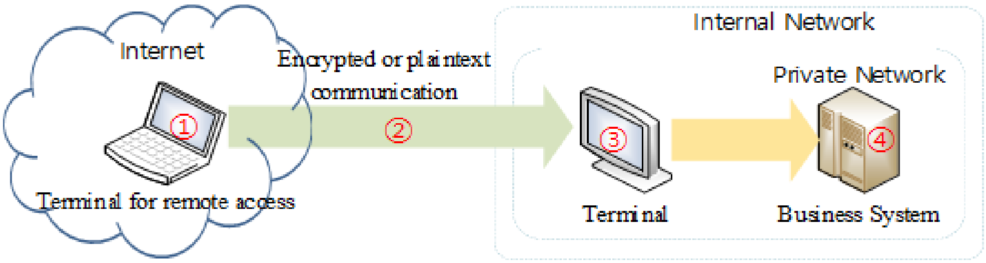


Fig. 4. Composition of the system using PC remote access program.

There are examples of cyber security incidents that occurred in the system configuration shown in **Fig. 4**, such as the case in which TeamViewer, a remote management and collaboration program, was attacked by Chinese hackers, and another hacking case in which pornography was exhibited on the screen in the course of a conference using the video conferencing service 'Zoom' in the South African Parliament.

2.1.5 Zero Trust security

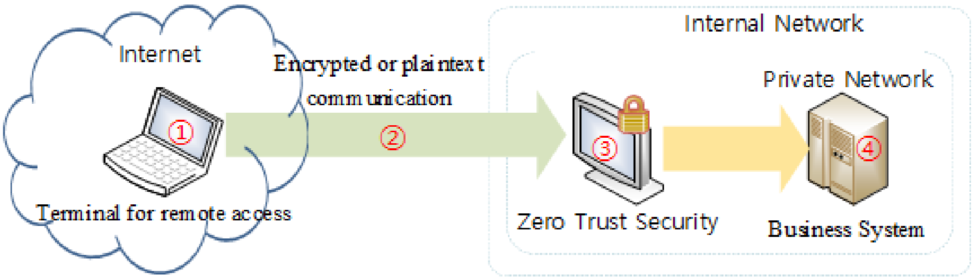


Fig. 5. Composition of the system using Zero Trust.

The Zero Trust security technology has not been allowed yet. With the Zero Trust technology, ① a terminal with verified reliability (whether internal or external network) can access the ④ work system of the internal network. As this method separates the networks according to the set level of trust without differentiating between internal and external networks, it cannot be used under the current network segregation regulations, in which there is a clear differentiation between internal and external networks. In addition, verification on security technology in terms of security performance and practical feasibility, which has been recently adopted for the work from home setup and use of the cloud service, is still insufficient. **Fig. 5** shows the system configuration using the Zero Trust security technology.

2.2 Problems for development of internet-based new technologies under the current network segregation environment

For development work of technologies such as open application programming interfaces (APIs) and distributed ledgers, increasingly adopted in the financial sector, developers typically use open source, which requires a seamless external network connection. However, after the implementation of network segregation, productivity for the development of internet-based new technologies such as in fintech companies has declined. In this regard, differentiated application of regulations is necessary. For instance, by assessing the level of risk according to the type and characteristics of work and the importance of user data, exceptions on the obligation of applying physical network segregation for some work can be applied.

However, although there is a definite necessity for differentiated application of network segregation regulations, there are various security threats that can arise in a non-face-to-face work environment, and the types of major security threats are listed in **Table 1**.

Table 1. Major cybersecurity threats that can arise at non-face-to-face work

Type	Characteristics
Physical threats	• In general, locations for remote work are not guaranteed as a secure working environment at the level of security provided by the company • There is a risk of equipment theft in cafes and libraries, places with unspecified crowd gatherings • There is a risk of loss or theft of business IT equipment while moving
Human threats	• As work is performed in a non-face-to-face manner, exposure to various social engineering attacks and unintended abnormal behaviors may occur • Company's business-critical data may be externally leaked through user terminals used for remote work • When working from home, family members, visitors, or children can access IT equipment for work and modify or delete data
Technical threats	• If a user's terminal is vulnerable to cyberattacks and infected with malware, the damage may spread due to the intrusion to the company's internal network by an unauthorized user • If the network environment used for remote work is not secure, communication content or data may be leaked • If the access authentication procedure of the information processing system for work is not strongly established, unauthorized terminals can access the internal network of the company

As an example, in October 2019, Avast, a cybersecurity software company, announced a network breach incident in a non-face-to-face environment. The malicious hacker obtained the

VPN account information of an employee used for remote work and succeeded in infiltrating the corporate internal network by exploiting a weak point in the security setup, in which multiple authentications were not required. The actual date of detection of intrusion was September 23, but evidence of intrusion attempts was found from April of the same year. Avast did not respond to the incident for 2 weeks to first determine the reason for the attacker's intrusion, and finally identified that the attacker's intention was to tamper with CCleaner, one of Avast tools. A similar intrusion incident was reported in 2017 [5].

In a non-face-to-face/remote work environment, the use of remote-access VDI terminal connected to the internet is unavoidable, which exposes users to various security threats as a consequence.

In addition, with the fast digital transformation across the industry, interest in the use of cloud service continues to increase to achieve business agility and efficiency in costs of IT infrastructure construction and operation. With more relaxed implementation of cloud-related regulations at present, the domestic cloud market is expected to become more active, and the interest and consideration on the adoption of cloud services have been increasing in line with the current tendency. In particular, Zero Trust technology, which has been currently reviewed for use in non-face-to-face/remote work environment, is more suitable for resolving security issues in cloud environments.

In general, cybersecurity incidents, such as deletion of data and backup files, and mass leakage of customer information may arise in cloud environment due to mistakes of a cloud service provider (CSP) or an administrator who manages the cloud service. In other words, a large number of security incidents are caused by CSP's carelessness or mistakes, or errors in setting or configuration.

Regarding alternative technologies for network segregation, measures for improving both the security and efficiency are under discussion. Depending on the data importance, network segregation is applied for confidential/critical data and otherwise excluded from the application target of network segregation. Thus, the security management is not centered on the network perimeter between the internal/external network.

As can be seen from the above discussion, when internet-based new technologies are used for development, as there are various security threats and corresponding implications, it is necessary to consider the method of implementing network segregation according to the importance of data as well as the security centered on internal/external network perimeter. Rather than applying a standardized network segregation regulation across all cases, a rational method should be derived by designing a network segregation application method and architecture according to each situation.

2.3 Problems with the application of network segregation from the viewpoint of fintech companies

Fintech is a compound word of finance and technology. Currently, fintech companies are making requests on deregulation of network segregation. This section describes the problems that arise when applying standardized network segregation to such companies.

As previously described, the limitations of network segregation, which makes the work environment inefficient and less productive and incurs excessive costs, have been addressed by fintech companies. Network segregation refers to financial security regulations that separate the communication lines of financial companies into internal and external networks to prevent cyberattacks and information leakage. These regulations have been established as a security policy after a hacking incident in a financial company in 2011. The regulations that fintech companies have addressed are the provisions in Article 15 of the Regulation on

Supervision of Electronic Financial Businesses, which refer to preventive measures for incidents such as hacking for financial companies or electronic financial companies. The specific parts are paragraphs 1 (3) and (5) of Article 15. These provisions impose that networks for internal systems and for operation or development of information processing systems are prohibited from accessing internet. **Fig. 6** illustrates the physical and logical network segregation.

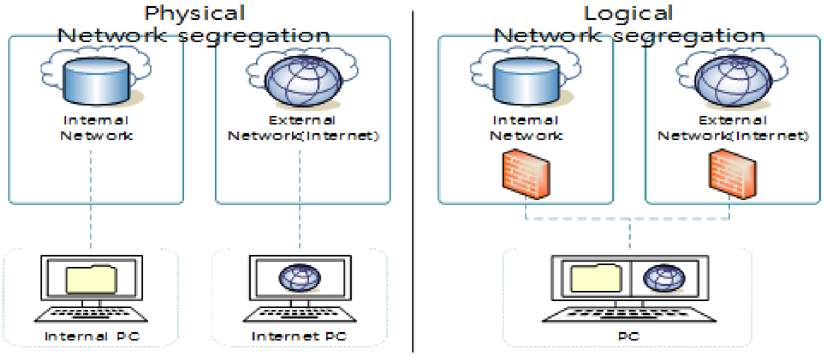


Fig. 6. Physical and logical network segregation.

The first problem addressed by fintech companies from applying standardized and undifferentiated network segregation is the problem of reduced work productivity. With the separation of the internal network and internet, it is difficult to implement a cloud-based platform. Thus, data received via internet by e-mail need to be copied or resent to the work PC to be used, requiring additional and unnecessary procedures and thereby delaying the work process. This poses a serious productivity problem, particularly for developers. For example, even for cases when they try to use GitHub, a software development collaboration platform, individual manual work is required for open source code acquired by internet, or for transmission to work PC, and specific additional procedures are required for the code transfer, decreasing productivity. The Startup Alliance has recently released the 'Issue Mini-Summary' report [6], which indicates that the decrease in work productivity can reach 50% due to network segregation regulations. To compensate for the deceleration of the development progress, there are cases in which labor costs in the development sector were increased by 30% or more. According to a recent survey by the Korea Fintech Industry Association, more than 88% of member companies agreed to the deregulation of network segregation, and the basis for this opinion was mainly the decrease in work productivity and the cost burden.

3. Cases of regulations and applications of internal network protection technology: overseas cases in financial sector and domestic cases in non-financial sectors

3.1 Cases of regulations and applications of internal network protection technology in overseas financial sectors

This section describes cases of regulations and application of internal network protection technology related to the financial sector in other countries. The cases of Russia, the United Kingdom (UK), the United Stated (US), Europe, and Australia are described as follows.

- Russia [7]

For protection of their banking system, the Russian financial sector has mandated: 1) the establishment of in-house standard by financial companies; 2) control on the access to internet resources and transmission/receipt of data; 3) blocking of unauthorized internet use. In addition, to reduce the threats in internet communications, technical protective measures have been implemented, such as firewalls, anti-virus tools, intrusion detection, and data encryption. Physical network segregation for the internal network is not mandatory, but it is one of their recommendations.

- UK [8]

In the UK, through the Financial Services Act enacted in 2012, the Financial Conduct Authority (FCA) was established to oversee the overall business activities of the capital market. The FCA established a security policy for electronic finance businesses and presented it in a handbook. In particular, in the Financial Crime Guide [9] and Financial Crime Thematic Reviews [10], security measures have been proposed, such as designation of administrators for data protection, monitoring of the external service providers, access control for data, user account management, risk-based monitoring, use of strong passwords and prohibition of sharing the passwords, and management of removable storage media. In these guidelines, a strong policy of blocking internet such as network segregation has not been recommended, but it is specified that internet and email access should be allowed only for employees who need the access for work. The guidelines also address the blocking of internet contents.

- US [11]

The US Federal Financial Institutions Examination published an IT Handbook for financial inspection. Regarding the information security sector, policies regarding IT inspection are specified for directors of financial institutions for internal network protection. Each policy addresses access control and application security for computer networks. For network access control, it is necessary to set security zones according to appropriate requirements to control access within or between security zones. For protection of applications connected to internet, abnormal access to different zones should be blocked through network segregation. It is stipulated in the handbook that financial institutions must implement a network access control system for detection of abnormal access from unauthorized devices, maintain and manage an accurate network diagram and data flow chart, and implement adequate controls for wired/wireless networks. However, there is no explicit recommendation on network segregation.

- Europe [12]

The European Banking Authority established guidelines to ensure that financial companies comply with the requirements related to ICT and security risk management. The guidelines stipulate that financial institutions must implement procedures for prevention of security problems in ICT systems and ICT services, thereby minimizing the impact on the provision of ICT services. In addition, financial institutions must continually make decisions on whether the changes in the existing operating environment affect security measures, or whether there is a need for additional measures for optimal supplementation, and ensure these measures are optimally implemented. As measures to reduce the ICT and security threats, financial institutions must perform composition of organization, logical security, physical security, ICT operation security, security monitoring, information security re-check, guidance, and education. Among these, in ICT operational security, restriction of unnecessary traffic through appropriate network segmentation has been stipulated, but there is no explicit requirement on network segregation.

- NIST [13]

Special Publication 800-53 by the National Institute of Standards and Technology (NIST), US, addresses 'Security and Privacy Control for Federal Government Information Systems and Organizations.' This document aims to provide assistance for US federal information systems in all fields other than defense such that they can comply with information security laws and regulations with clarity and efficiency. Out of 18 areas of control, in System and Communications Protection, implementation of network segregation/network segmentation is recommended for the public sector. Aspects such as “which information, for what purpose or functions” have been left up to the discretion of respective organizations.

As shown in the cases discussed, major cases such as Russia, the US, the UK, and the European Union have institutionally established security policies similar to Regulation on Supervision of Electronic Financial Businesses of South Korea to ensure the stability of electronic financial businesses and transactions. In these policies, basic information security requirements that should be applied by financial companies are stipulated. There are common requirements such as prohibition of granting unnecessary access rights, blocking unnecessary communication by network segmentation, controlling the user accounts and access. Although a number of countries including Russia recommend the implementation of network segregation, no country has institutionally mandated network segregation, as in the case of South Korea.

3.2 Network segregation for protection of the internal network of governmental and public agencies

With the increasing number of cases of external leakage of important business data due to cyberattacks such as hacking, network segregation was adopted to establish a safe work environment, in which the access to business-related information through internet is blocked by separating internal network at work and internet (external network).

Network segregation of governmental and public agencies is based on the Basic Guidelines of National Information Security by the National Intelligence Service, and detailed procedures for network segregation are specified in a separate guideline.

According to this guideline, when governmental and public agencies plan to introduce network segregation, they are required to follow the following procedures: ① information system identification, ② decision on the information system domain (decision on internal/external network), and ③ network configuration. When deciding on the domain of an information system, it is necessary to understand the characteristics of the business in which the information system is used, and to determine the importance of information produced, managed, and operated by the information system.

In addition, the domain in which the information system should be located must be carefully considered before the decision, because the determined domain would have a considerable impact on the flow of information, and influence the efficiency and appropriateness of work.

According to the criteria in **Table 2**, the domain of information system is classified into internal network at work and internet. The information system classified by these criteria is divided into a business network and an internet network, and the overall network configuration is as shown in **Fig. 7**.

Table 2. Criteria for determining the information system area

Work/information importance	Description	Remark
Group 1	Information systems related to information that may have a critical impact on national security and national interests and should not be publicly disclosed.	Internal network at work
Group 2	Information system related to information that is important for the operation and management of the country, and may cause confusion if publicly disclosed.	Internal network at work
Group 3	Information system related to information regarding public service support, which should be publicly disclosed and externally utilized	External network

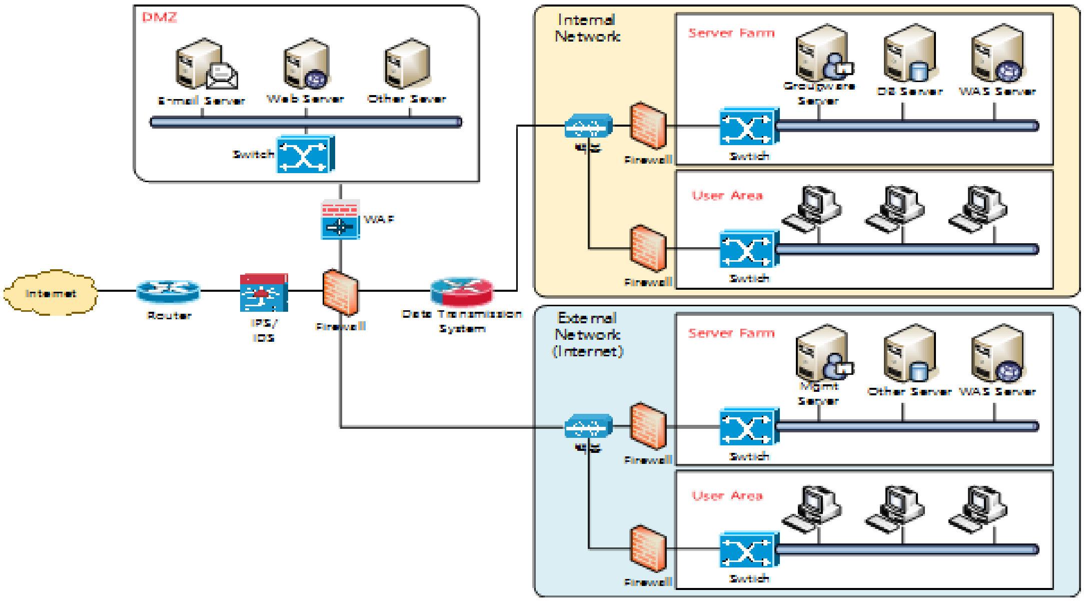


Fig. 7. Detailed composition of physical network segregation.

4. Proposal for rationalization of network segregation regulations

From the cases mentioned, the current status of network segregation implemented in the non-financial sector in South Korea was examined through cases of network segregation implemented to governmental and public agencies and ICSs. Governmental and public agencies and ICSs classify the target of network segregation application based on the importance of the system and data, and accordingly define the installation domain of the system as an internal or external network. In contrast, the network segregation policy implemented in the financial sector simply defines how to access the internal network from the outside, resulting in various problems. Improvement measures for these problems will be discussed in the following section.

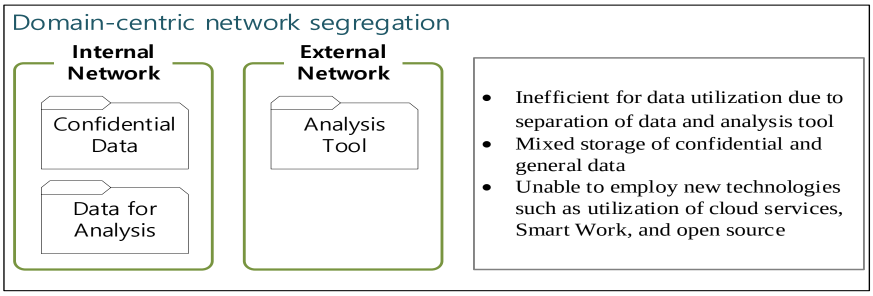
In addition, FSS allows exceptions through the “application for non-implementation” whenever new environmental changes and requirements emerge, and this process is repeated. Therefore, in this section, for reasonable resolution of the network segregation regulation in South Korea's financial sector, we propose 1) the introduction of a data classification system for transformation to data-centric network segregation policy, 2) a standard security model for remote work/working from home setup when network segregation is applied, and 3) alternative control measures when network segregation is not implemented.

4.1 Introducing a classification system for data-centric network segregation

The current "network segregation" policy was indicated as one of the regulations that needs to be improved and revised in the "recommendations for the government." Thus is a document presenting the outcomes of the activities of the Presidential Committee on the 4th Industrial Revolution, an organization established for the introduction of the 4th industrial revolution in South Korea. The core content of the cybersecurity area was that "the cybersecurity policy should be transformed from the existing domain-centric policy to a data-centric policy," and the network segregation policy was indicated as a representative example of the current domain-centric security policy. This is because the current policy contradicts the basic philosophy of the 4th Industrial Revolution that "everything is connected to the network, and data must be actively shared and utilized," and it acts as an obstacle to fostering and growth of related industries. Therefore, seeking a transformation of the cybersecurity policy according to the level of data importance is imperative. To this end, as a priority, an electronic data classification system based on data importance must be developed, and based on this classification system, the network segregation policy needs to be re-established according to the level of data importance.

The development of a data classification system precedes the transition to this data-centric cybersecurity policy. Accordingly, when new information is produced in an organization, it is necessary to prepare a data classification system that can be processed in the order of "type classification → grade classification (importance) → security service response." As for the method of classifying the type and grade of data, it is considered that a number of prior studies can be used, including the government-wide data reference model and NIST SP800-53 [13].

Through establishment and implementation of a data classification system, it is possible to improve the problems of domain-centric network segregation shown in Fig. 8, and shift to a data-centric network segregation policy (Fig. 9). Thus, problems arising from the introduction of new internet-based technologies such as fintech and clouds could be addressed while retaining the network segregation policy.



- Inefficient for data utilization due to separation of data and analysis tool
- Mixed storage of confidential and general data
- Unable to employ new technologies such as utilization of cloud services, Smart Work, and open source

Fig. 8. Limitations of current domain-centric network segregation system implemented in South Korea.

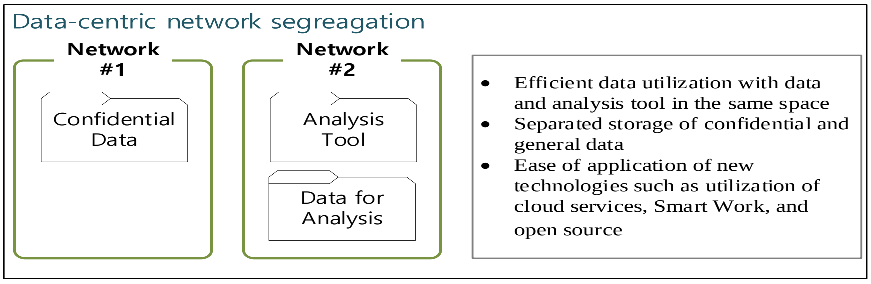

Data-centric network segreagation
Network #1
Confidential Data
Network #2
Analysis Tool
Data for Analysis
Efficient data utilization with data and analysis tool in the same space
Separated storage of confidential and general data
Ease of application of new technologies such as utilization of cloud services, Smart Work, and open source

Fig. 9. Types and advantages of data-centric network segregation.

4.2 Proposal of standard security model for remote work

Due to COVID-19, the implementation of working from home setup has been expanding, and the demand for remote work/working from home, which requires exceptions to the application of network segregation due to the changes in working method, is increasing. Thus, deregulation of network segregation regulations is required. However, as the introduction of remote work/ working from home setup can disable security control through network segregation and may cause problems, as shown in **Table 3** [14], security measures are required.

Table 3. Major security threats from remote work/working from home

Category	Major security threats
Inadequate physical control of external terminals	• When an external terminal used for remote work is lost or stolen, or when other people peek into the information, data in the terminal is leaked or exposed • Unauthorized internal network access through external terminal
Use of network without security verification	• Leakage of important information due to tapping or MITM attack when accessing the internal network through a shared wired or wireless network
Network intrusion following malware infection	• Possibility of system intrusion when the internal network is connected through an external terminal infected with malware
Threats of remote access to the internal resources	• Security threats such as unauthorized access as external terminals can access internal resources that were previously accessible only from inside

Accordingly, as shown in **Table 4**, FSS stipulates matters for information security controls in case of remote access for remote work/working from home setup as provisions in Detailed Enforcement Regulations on Supervision of Electronic Financial Businesses. In the “Guide on security of working from home system for financial companies,” considerations according to the type of remote access have been presented [15]. In this guide, remote access has been classified into “direct access” and “indirect access.” For “direct access,” direct connection to the internal network of a financial company is permitted and protective measures equivalent to the terminals physically located inside the financial company are required. In addition, two methods of “indirect access” are proposed in the guide: methods of VDI and remote access program. However, as previously mentioned, remote access has various weaknesses, and it is highly likely that the network segregation policy for protecting the internal computer network will be disabled. “Direct access” indicates directly connecting the internal network from the outside, and unless a terminal provided by the company and a dedicated line are used, network segregation will not effectively operate.

Table 4. Controls for information protection as alternatives to network segregation

Category			**Items of control**
Common application			• Diagnosis and recovery of malware infection by targeting electronic data transmitted from external to internal network • Establishment and application of blocking measures for advanced persistent threat • Establishment and application of measures of detecting, blocking, and follow-up monitoring of information leakage when electronic data is transmitted outside
Email system			• Establishment and application of measures to prevent malware infection through e-mail including the text body and attachments • Establishment and application of measures of detecting, blocking, and follow-up monitoring of information leakage through e-mail
Terminals for work			• Removing administrator rights of the user • Establishment and application of measures to install and execute only authorized programs • Encryption for electronic data storage
Remote access	External terminal	Common application	• Antivirus program installation, real-time update, and inspection • Use of safe OS and application of the latest security patch • Setting login password and screen saver • Applying measures to prevent information leakage due to screen images and print-outs
		Indirect access	• Blocking transmission/reception of files between external and work terminals
		Direct access	• Blocking unauthorized software installation • Blocking arbitrary changes to security settings • Blocking read/write function of external storage devices such as USB • Encrypted storage of electronic data (files, documents) • Applying measures to prevent information leakage when the terminal is lost (e.g., hard disk encryption, application of CMOS password)
	Internal network access control		• Connection is allowed only for IPs and ports essential for business • Recording and saving information on remote access (e.g., accessor ID, date of access, access system)
	Authentication		• Application of double authentication (e.g., ID/PW + OTP) • Blocking access when authentication fails more than a set number of times (e.g., 5 times)
	Communication line		• Encrypt network section with secure algorithm • Blocking internet connection when accessing the internal network (however, internet connection is always blocked for remote access terminals directly connected to the internal network) • Blocking network connection when a set idle time elapses after remote access
	Others		• Request a security pledge for remote accessors • Ban remote access in public places

In addition, the Bring Your Own Device terminal used for “indirect access” can be exposed to malware infections due to difficulties in application of forced security controls from the financial company, and thus it is necessary to provide supplementary measures. There is no standard model for building a remote access system in compliance with the “alternative control measures on information protection without application of network segregation,” which inevitably aggravates confusion and complexity for financial companies. Furthermore, the construction of remote work systems for each financial company requires considerable investment on the associated cost and manpower. Thus, in practice, it is difficult to build remote work systems for small-scale financial companies such as savings banks and mutual saving and finance companies. This is highly likely to lead to the construction of a remote work system vulnerable to hacking threats, and may emerge as a persistent problem in the future.

Therefore, the FSS needs to present a standard model for remote work environment in which financial companies should operate. In addition, if small and medium-sized financial companies are not able to build such an infrastructure, a plan is required to build and support a shared infrastructure that they can use jointly. For example, the Korean government has addressed these problems by establishing G-VPN and a mobile shared base that all central administrative agencies and local government agencies can use jointly.

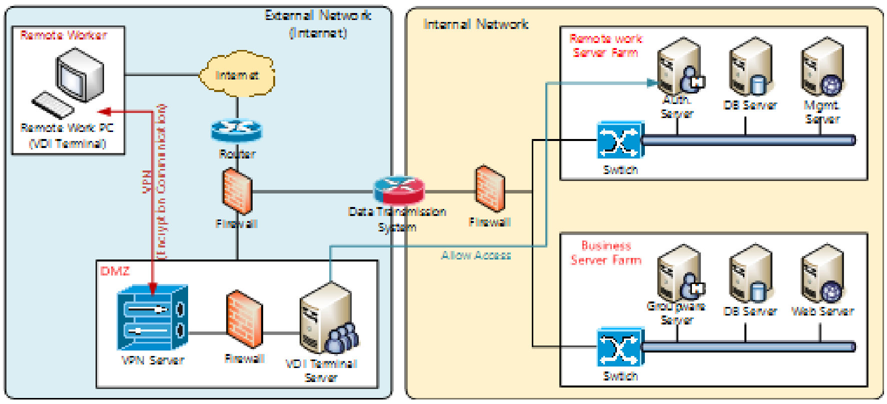


Fig. 10. Standard model for remote work system.

Fig. 10 presents a standard model of a remote work system that should be applied by financial companies. A VDI terminal server for working from home arrangement is built in the internet domain, and the remote worker should have access to the VDI server via a dedicated remote work terminal and access the work server in the internal network at work. In addition, the connection through the VPN server should be made only by the internet, and the internal network access through the VDI server should be allowed only through the inter-network data transmission system or a security gateway that has a similar function. This model cannot be applied to cases of 'direct access', and the use of the 'direct access method', which allows internet connection to the internal network, should be avoided. If the 'direct access' method needs to be used, the financial company's security policy should be fully applied to the connection terminal and this setting should not be permitted to change. For this purpose, the access terminal must be provided by the financial company. In addition, the applicable terminal must implement a function to access a VPN that facilitates access to the computer network of the financial company before any other network connection, as a priority.

Fig. 11 illustrates a model with a remote access terminal that can be used for indirect or direct access with application of all the security measures required in Table 4. In this model, 1) “VPN priority connection” is executed on a terminal constructed based on secure OS, which blocks access to all networks other than the network of the financial company, and 2) a virtualization software is used to boot Windows OS. Thus, secure network configuration is achieved while complying with terminal control measures.

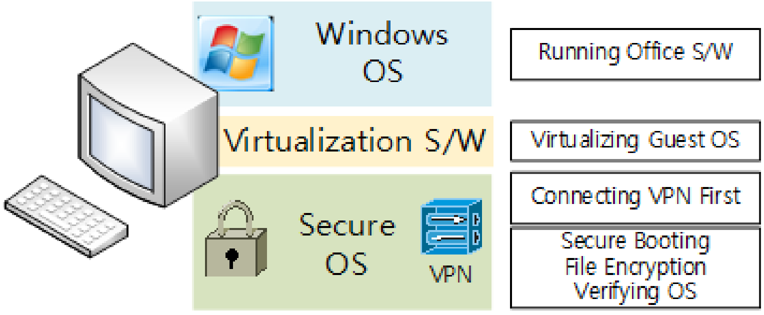


Fig. 11. Standard terminal model for remote work system.

4.3 Alternative control measures without application of network segregation

Zero Trust is a technology that can be used as an alternative control measure when network segregation is not implemented. This technology is a new concept in cybersecurity technology in which no accessor (terminal), regardless of the internal/external network, is trusted, and all users, devices, data, network flows are separated and connected only after the trust verification process is completed with strictly managed authentication procedure. By using Zero Trust technology, without differentiation between internal and external networks, a terminal with verified level of trust can access the work system of the internal network. That is, this method separates the network according to the level of trust regardless of the internal/external network status. For all access to the enterprise system, authentication, authorization, and encryption procedure are applied and access is available without differentiation between in/out of the company. In addition, network access control is possible only with a security policy without a separate connection procedure such as a VPN connection program. In all cases, access is allowed only when the safety of the device and the user have been completely verified. The process of applying Zero Trust technology is outlined as follows:

- Identification of sensitive data in storage or in transmission;
- Path mapping for access and transmission of sensitive data;
- Design with micro-segmentation and granular perimeter enforcement;
- Zero Trust environment monitoring through security analysis;
- Security process automation and adaptive response acceptance.

In establishing a system based on Zero Trust technology, data identification and classification are required. Organizations planning to implement Zero Trust technology should analyze all data/information flows and important data, and establish a separate access control policy for each type of data. For this, classification of data is required in advance. Therefore, under the current network segregation policy in the financial sector, immediate implementation of Zero Trust technology will be difficult, but data classification for data-centric network segregation policy is required as a prerequisite.

4.4 Comparison between the proposed method and legacy network segregation

Comparing the proposed improvement of network separation with the existing network separation policy applied to the financial sector, the following is a comparison.

1. Introduction of a data classification system for data-centric network segregation

The current network segregation policy is a standardized and undifferentiated security policy centered on the domain division between internal and external networks. Therefore, transformation to data-centric policy is required. Accordingly, transition of cybersecurity policy according to the classification of data importance is necessary. For this purpose, an electronic data classification system based on the level of data importance should be established as a matter of priority, and based on this classification system, network segregation policy should be re-established considering the data importance.

2. Proposal of standard security model for remote work

Since the COVID-19 pandemic, limitations on the implementation of working from home/remote work arrangement due to network segregation policy have emerged as one of the most pressing issues in the financial sector. In this regard, FSS has requested to comply with “alternative control measures without network segregation” and allowed remote work setup. However, the absence of a standard model for remote work system for financial companies to operate may lead to vulnerabilities in cybersecurity. Therefore, in this study, a standard model for establishing a remote work system and terminal security model with tighter control, which could be implemented in financial companies, is presented.

3. Alternative control measures without application of network segregation

Zero Trust is a technology that can be applied as an alternative control measure when network segregation is not implemented. This technology is a new concept in cybersecurity technology in which no accessor (terminal), regardless of the internal/external network, is trusted, and all users, devices, data, network flows are separated and connected only after the trust verification process is completed, with a strictly managed authentication procedure. However, to implement Zero Trust technology, a shift of policy from domain-centric to data-centric network segregation is required. Further review and evaluation for alternative security measures including Zero Trust technology are also necessary.

5. Conclusion

Network segregation policy refers to measures of blocking connection that separates the internal network at work and the external internet network to block unauthorized access and leakage of internal information through the external internet network. There are logical and physical network segregation methods to implement network segregation. Although the implementation of this policy has been effective in preventing information leakage and security incidents by total blocking of the source of external hacking and malware infection, it is necessary to improve the current network segregation policy according to the demands of the times such as necessity for remote work arrangement and adoption of new technologies. Accordingly, in line with the direction of supervision of IT in financial sector, to “establish an autonomous financial security system” based on technology neutrality and risk assessment that is principle-oriented, it is necessary to 1) rationalize network segregation regulations, 2) evaluate alternative technologies to network segregation and security performance of these technologies, such that autonomy can be granted for financial companies in their determination on the scope of network segregation application and methods of alternative control. This will facilitate the establishment of rationalization measures for network segregation policy implementation in the financial sector in South Korea. In response to this, it has been discussed that the financial sector in South Korea is the only case in the world that institutionally mandates implementation of network segregation, which leads to excessive and unnecessary waste in material and human resources across the financial industry. Furthermore, the network segregation regulations serve as obstacles to the adoption of IT-based new technologies in the sector, and the development of innovative financial businesses. In addition, it has been reported that there are cases of abandon of innovative ideas due to network segregation regulations in the fields of financial industry. If forced implementation of network segregation cannot be abolished, the regulations should be revised to accommodate the demands for autonomy and accountability of financial institutions, which would be in line with the future development of the security industry.

Therefore, in this study, we first diagnosed the problems of network segregation application in the domestic financial sector, such as establishing a remote access system for working from home arrangement, utilization of internet-based new technologies, and implication of applying network segregation for fintech companies. Second, regulations and cases of application related to internal network protection technology in overseas financial sector were investigated. Based on the analysis, rationalization measures for the network segregation regulation were proposed, which would require policy decisions to reflect these rationalization measures.

The findings of this study confirmed that the undifferentiated implementation of network segregation is hindering the innovative development of the financial sector. To overcome this, deregulation of network segregation policy in line with current tendencies and demands is necessary. In this regard, this study presented rationalization measures for network segregation regulation. Based on these findings and proposals, we aim to contribute to the seamless development of the financial sector in South Korea.

References

[1] J. Y. Park, Y. S. Jung, and J. W. Lee, “A Study on the Status of Network segregation and Policy Improvement in Financial Sector,” *The Korea Institute of Information Security and Cryptology*, vol. 26, no. 3, pp. 58–63, Jun. 2016. Article (CrossRef Link)

[2] J. Y. Kim, H. J. Kim, and C. S. Park, and M. J. Kim, “Analysis of Virtualization Technology Vulnerabilities in the Cloud Computing Environments,” *The Korea Institute of Information Security and Cryptology*, vol. 19, no. 4, pp. 72–77, Aug. 2009. Article (CrossRef Link)

[3] M. C. Novak, “How VDI Security Can Offer Your Business Peace of Mind,” May. 2020. Article (CrossRef Link)

[4] S. Khandelwal, “Qualcomm Chip Flaws Let Hackers Steal Private Data From Android Deviced,” Nov. 2019. Article (CrossRef Link)

[5] ZDNet, “Avast: No plans to discontinue CCleaner following second hack in two years,” Oct. 2019. Article (CrossRef Link)

[6] Startup Alliance, “Issue Minni-Summary : Network separation of FinTech companies,” vol. 1, Feb. 2020. Article (CrossRef Link)

[7] Bank of Russia Standard, “Maintenance of Information Security of the Russian Banking System Organisations,” Jun. 2014. Article (CrossRef Link)

[8] Financial Conduct Authority, “FCA Hand Book”. [Online]. Available: https://www.handbook.fca.org.uk/handbook

[9] Financial Conduct Authority, "Financial Crime Guide: A firm's guide to countering financial crime risks (FCG)," [Online]. Available: https://www.handbook.fca.org.uk/handbook/FCG.pdf, Accessed on: Dec. 2020.

[10] Financial Conduct Authority, "Financial Crime Thematic Reviews," [Online]. Available: https://www.handbook.fca.org.uk/handbook/FCTR.pdf, Accessed on: Dec. 2020

[11] FFIEC, "FFIEC Information Technology Examination Handbook: Information Security," [Online]. Available: https://ithandbook.ffiec.gov/it-booklets/information-security.aspx, Accessed on: Sep. 2016.

[12] European Banking Authority, "Guidelines on ICT and security risk management," Nov. 2019. Article (CrossRef Link)

[13] NIST, "NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organizations," Sep. 2020. Article (CrossRef Link)

[14] NIST, "NIST Special Publication 800-46 Revision 2: Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security," Jul. 2016. Article (CrossRef Link)

[15] Financial Security Institute, "Guide on security of working from home system for financial companies," Dec. 2020. Article (CrossRef Link)

Manyong Choi is a student in Ph.D course at Dept. of Computer Engineering in Ajou University, Republic of Korea. He received the master's degree from Hallym University, Republic of Korea. His research interests include Government information Security policy and analysis of Hacking Organizations Behind the State

Jin Kwak is a professor at Dept. of AI Convergence Network and Dept. of Cyber Security in Ajou University, Republic of Korea. He received the Ph.D. degree from SKKU, Republic of Korea. His research interests include Copyright protection, Cryptographic protocols, Applied security mechanisms for cloud and big data system and so on.